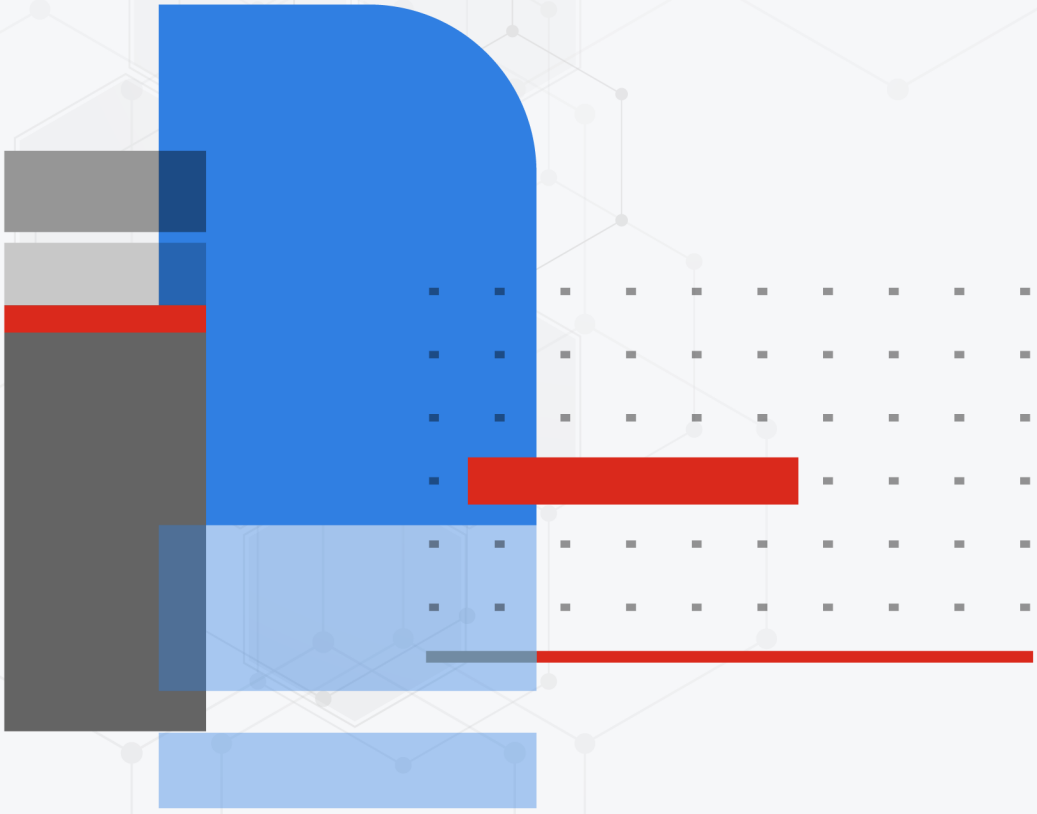
New Features Guide

FortiManager 7.4.0



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

June 20, 2023
FortiManager 7.4.0 New Features Guide
02-740-898074-20230831

TABLE OF CONTENTS

Change Log

Date	Change Description
2023-05-15	Initial release.
2023-06-20	Added: • FortiManager used as single-pane management tool to orchestrate FortiGate deployment in AWS on page 105 • FortiManager imports EPGs entries using the Cisco ACI connector as individual objects on page 140 • FortiSwitch replacement procedure can be executed from FortiManager GUI on page 54 • Support for IoT Virtual Patching in NAC policies using pre-built severity filters on page 82
2023-08-31	Initial release of FortiManager 7.4.1.

Overview

This guide provides details of new features introduced in FortiManager 7.4. For each feature, the guide provides detailed information on configuration, requirements, and limitations, as applicable.

The FortiManager new features are organized into the following categories:

For a list of all features organized by the version number that they were introduced, see Index on page 144.

Device Manager

This section lists the new features added to FortiManager for the device manager:

Device and Groups

This section lists the new features added to FortiManager for devices and groups:

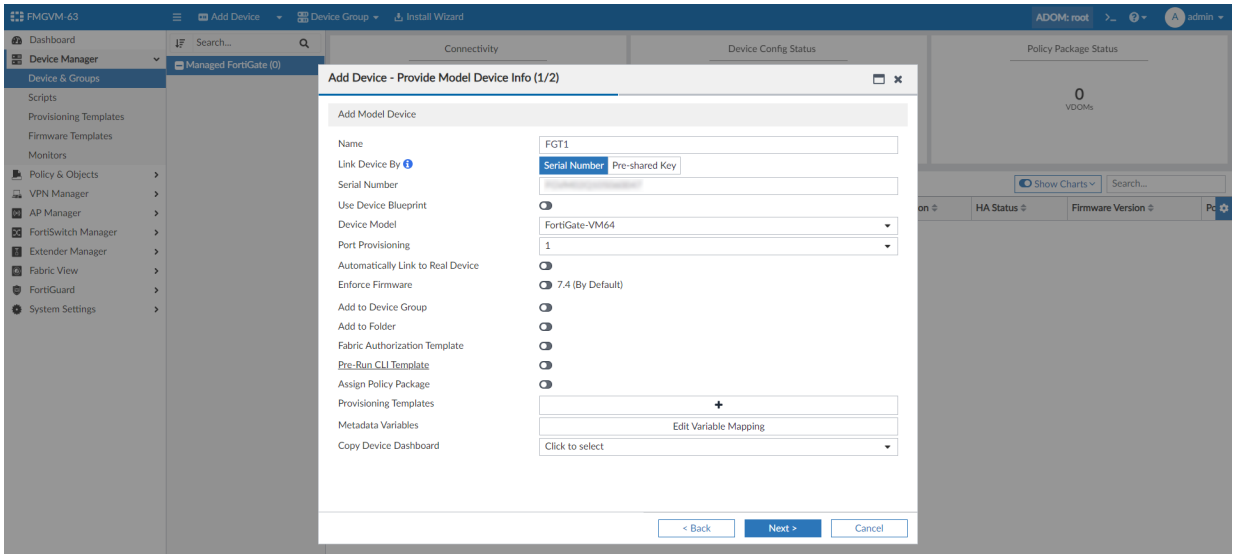
Auto-link setting is exposed to control configuration installation during ZTP - 7.4.1

This information is also available in the FortiManager 7.4 Administration Guide:
- Adding offline model devices
- Adding a model FortiGate HA cluster

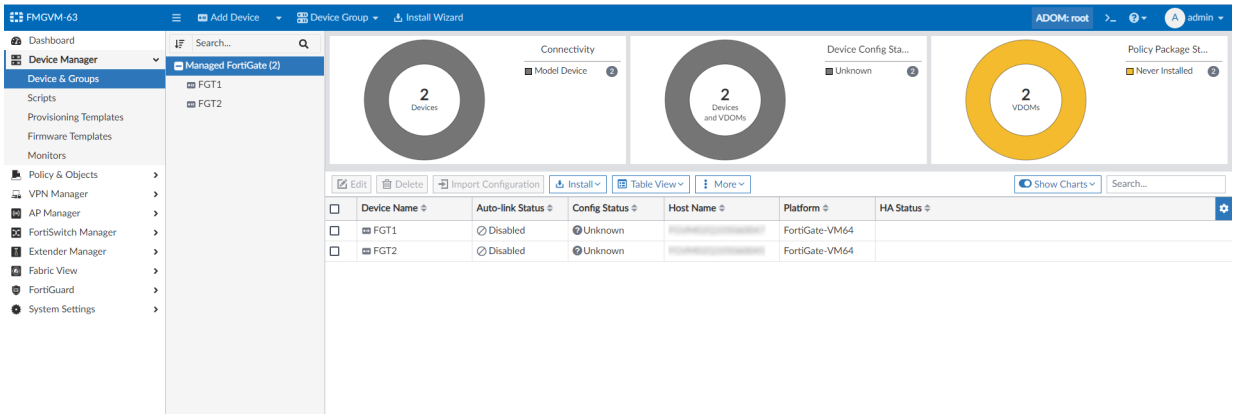
The auto-link setting is exposed in the model device wizard to allow administrators to better control configuration installation during the ZTP process.

To configure the auto-link setting for ZTP:

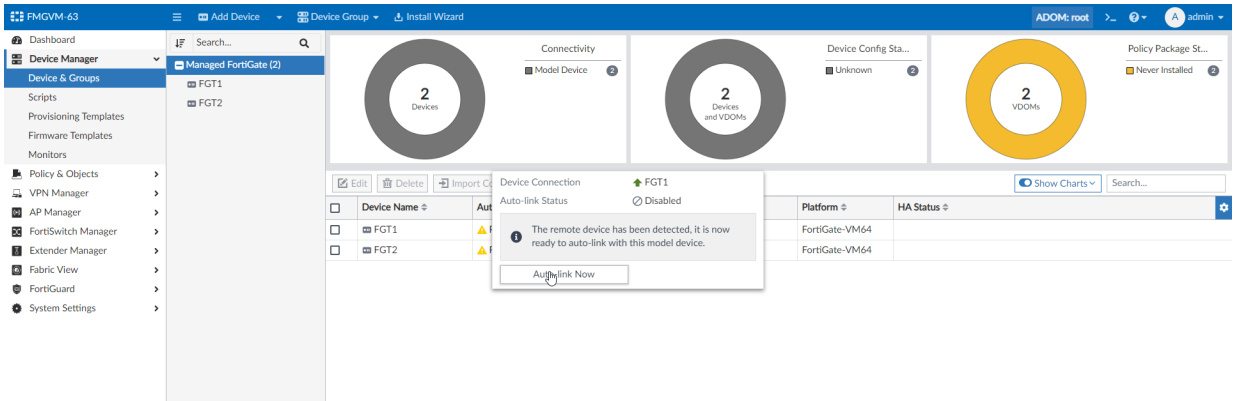
1. In the *Add Model Device* wizard, the option to *Automatically Link to Real Device* can be disabled or enabled.

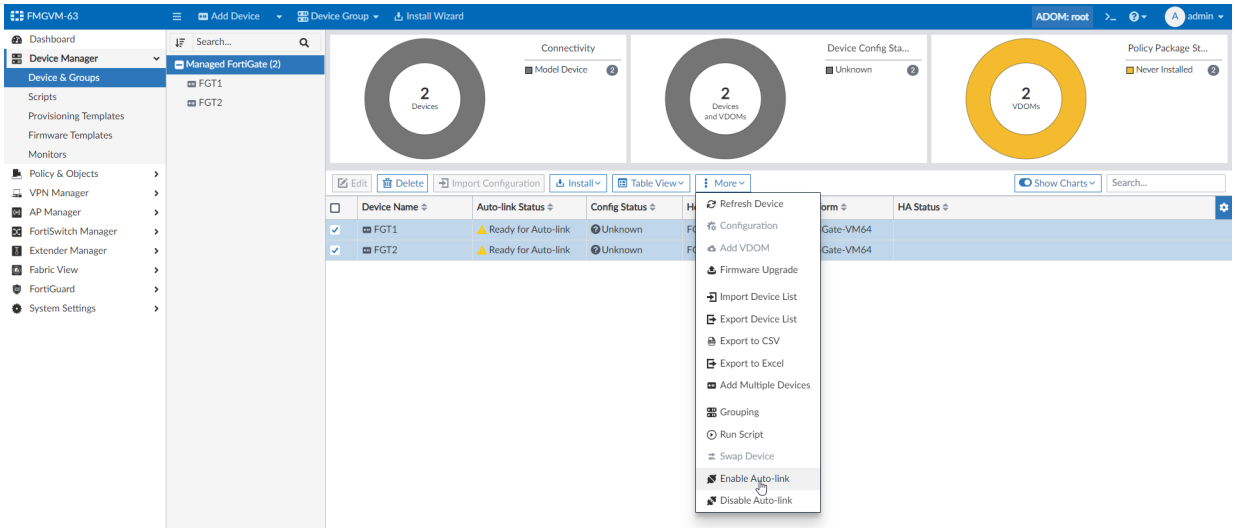


2. The auto-link status is displayed in the *Device Manager*.

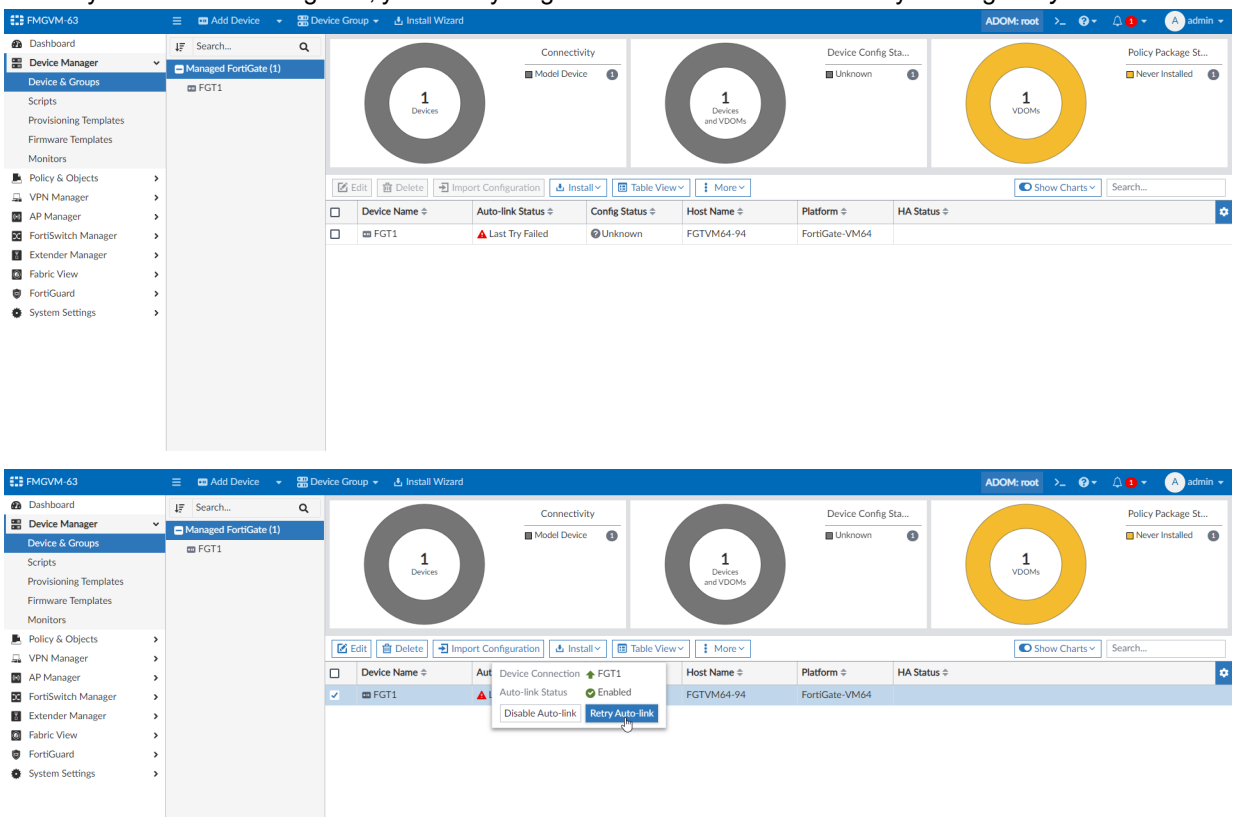


3. Auto-link can be enabled from the tool tip for single device, or by choosing multiple devices and selecting the *Enable Auto-link* setting in the *More* dropdown menu.

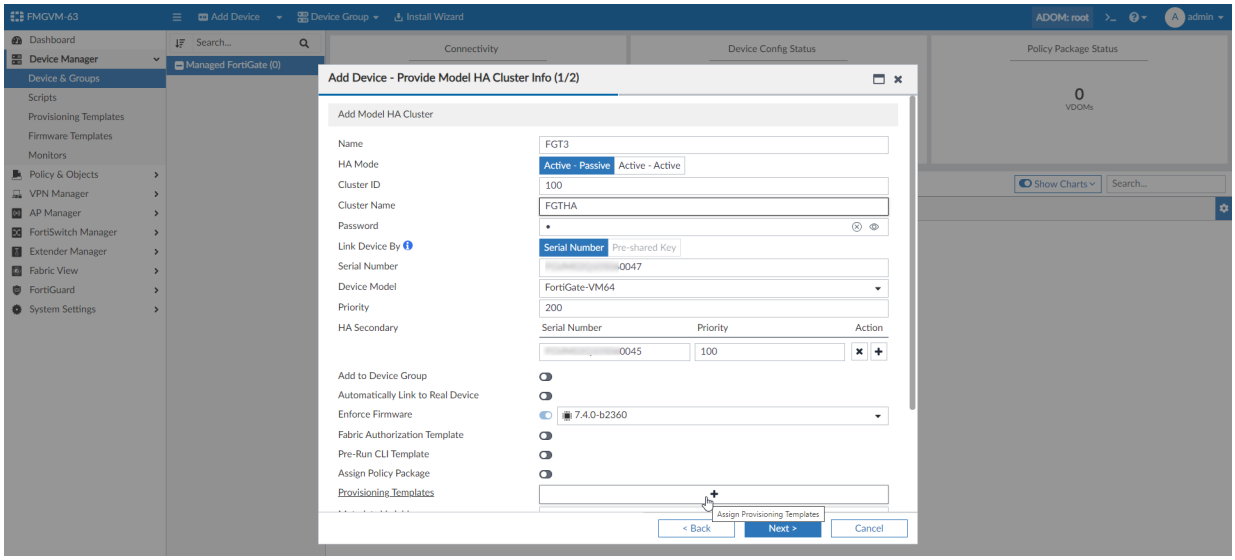


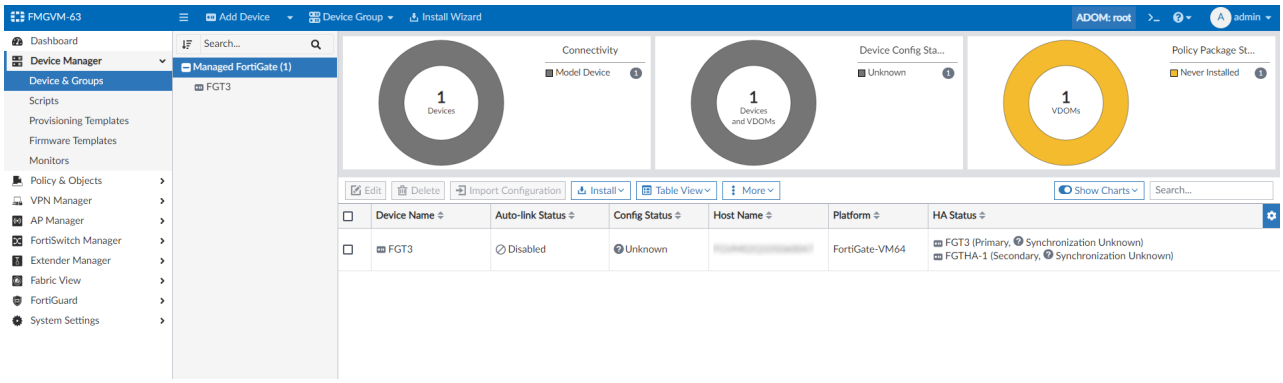


4. If for any reason auto-linking fails, you can try it again after the issue is resolved by clicking *Retry Auto-link*.

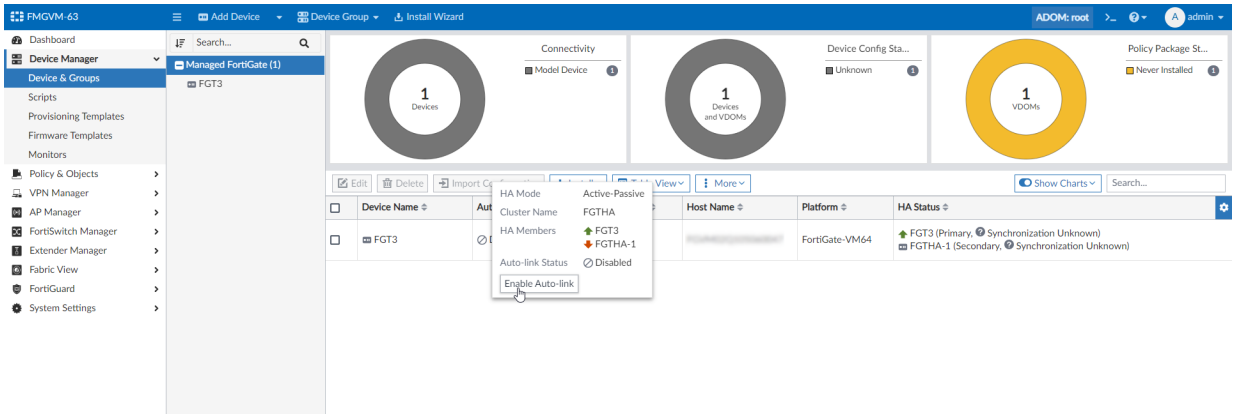


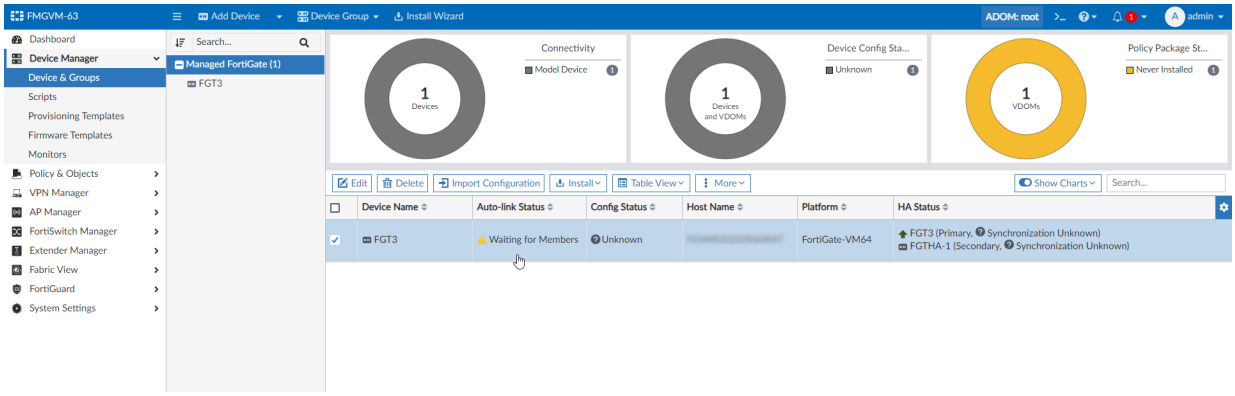
5. In the Add Model HA Cluster wizard, the option to *Automatically Link to Real Device* can be disabled or enabled.





6. After auto-linking is enabled, auto-link will be started after all cluster members are connected.





SD-WAN

This section lists the new features added to FortiManager for SD-WAN:

- Automated SD-WAN post overlay process creates policies to allow the health-checks traffic to flow between Branch and HUB on page 12
- Automated SD-WAN overlay process adds "branch_id" meta variable auto assignment on page 15
- SD-WAN monitoring map integrates with Cloud Assisted Monitoring Service to allow FortiGate interface speed tests from inside FortiManager on page 16

- SDWAN monitoring map enhancements on page 19
- SDWAN template for heterogeneous WAN link types on page 23

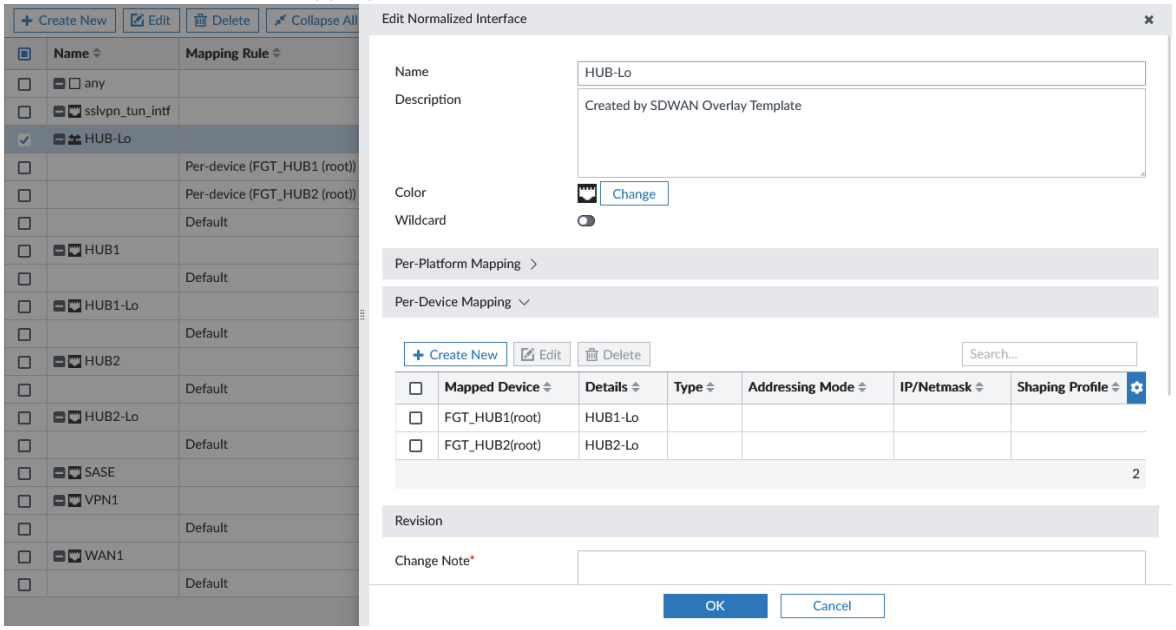
Automated SD-WAN post overlay process creates policies to allow the health-checks traffic to flow between Branch and HUB

This information is also available in the FortiManager 7.4 Administration Guide:
- Configuring an SD-WAN overlay template

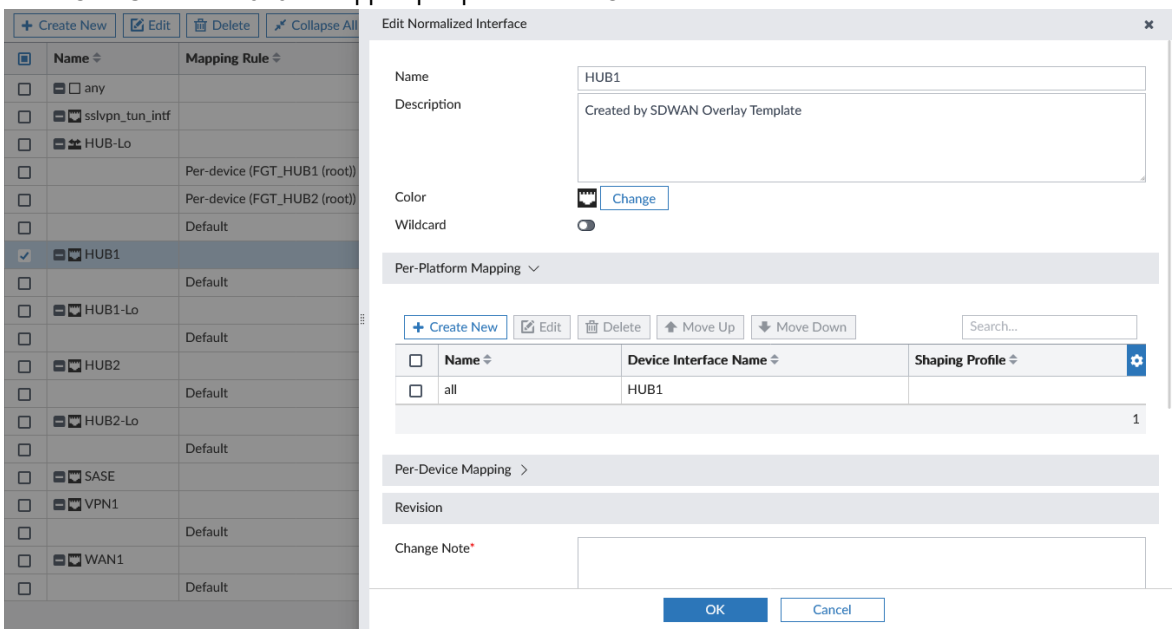
Automated SD-WAN post overlay process creates policies to allow the health-checks traffic to flow between Branch and HUB.

The SD-WAN overlay template includes two new options in the wizard to automate the post-wizard processes. The SD-WAN overlay template example configured in this document uses a dual-hub topology.

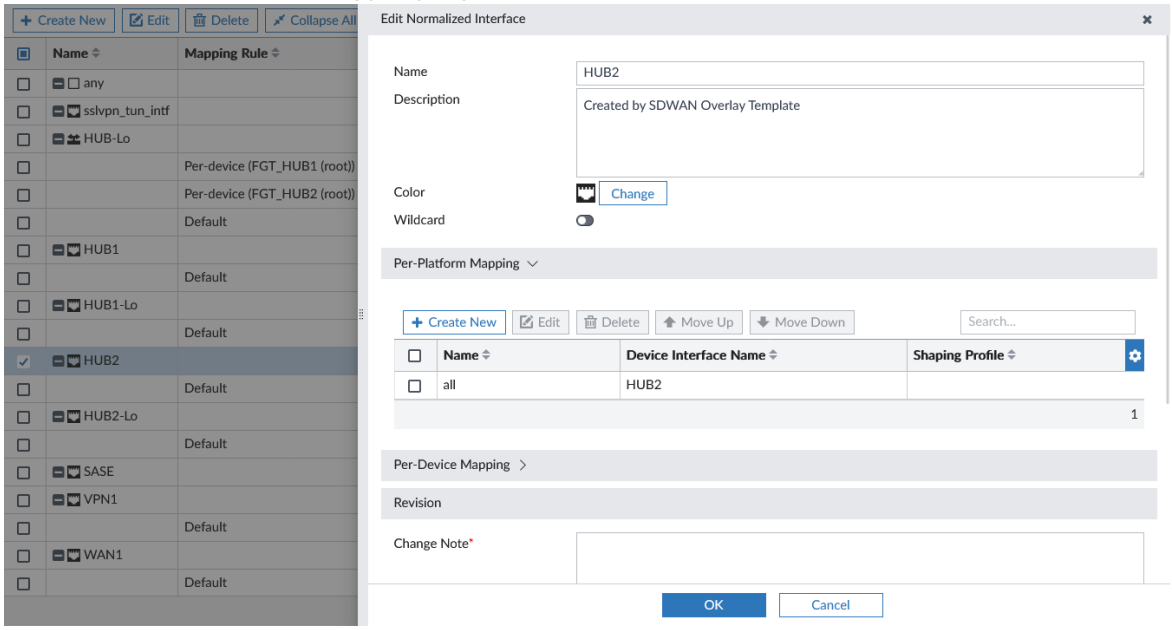
1. **Normalize Interfaces**
   Enable the *Normalize Interfaces* option to normalize the SD-WAN zones created by the template.
   - The following normalized interface is created for the SD-WAN Hub(s):
     - *HUB-Lo* with *Per-Device Mapping* to *HUB1-Lo* for the HUB 1 device and *HUB2-Lo* from the HUB 2 device.



- The following normalized interfaces are created for branch devices:
  - The *HUB1 SD-WAN zone* is mapped per-platform to *HUB1*.

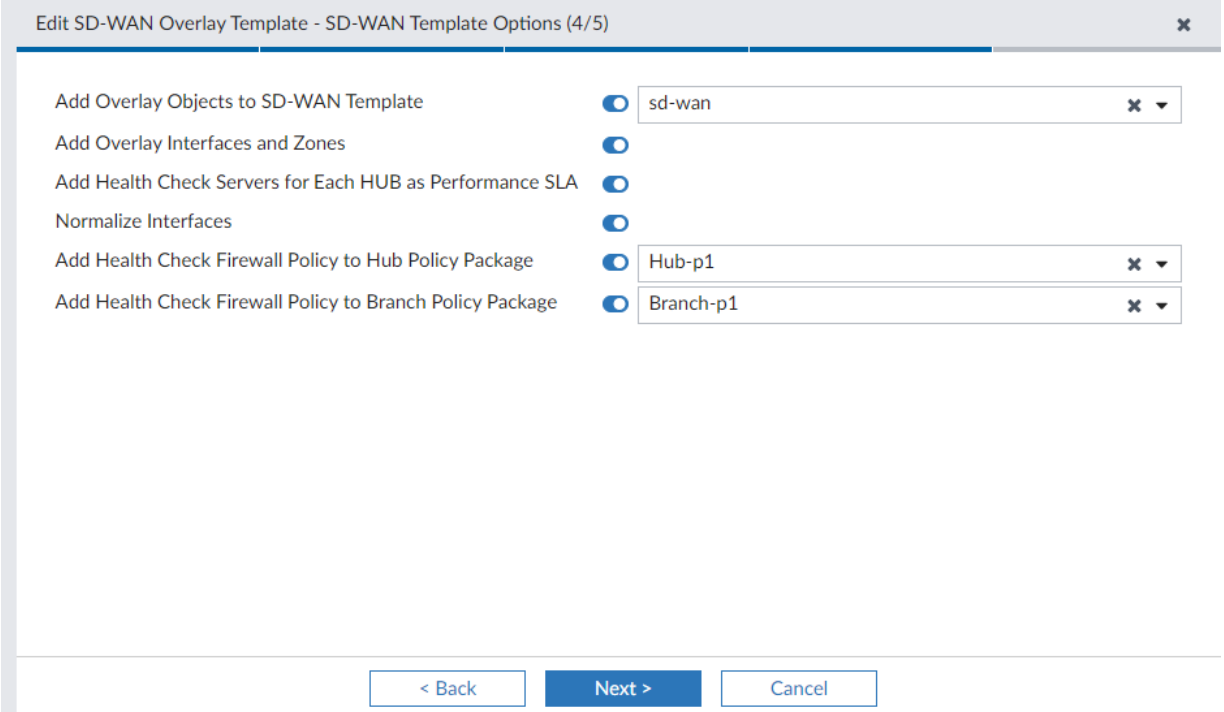


  - The *HUB2 SD-WAN zone* is mapped per-platform to *HUB2*.

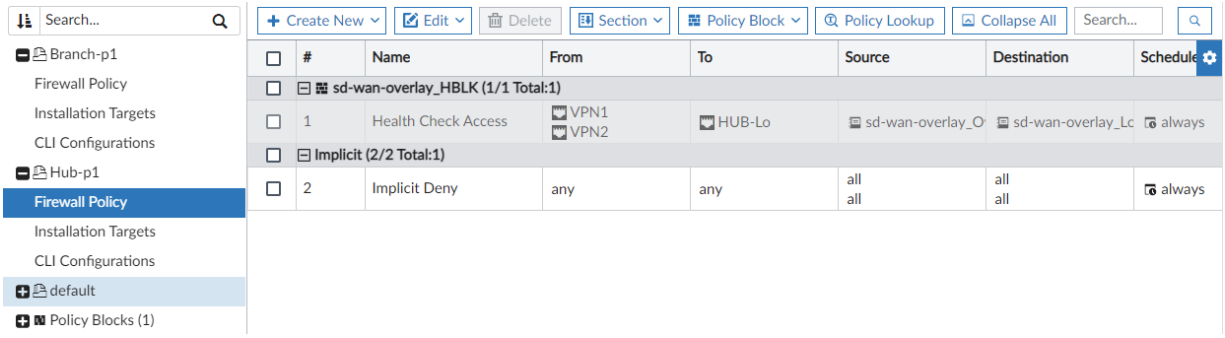


  - VPN IPsec tunnel templates are created for HUB interfaces when using the SD-WAN overlay template. When *Normalized Interface* is enabled, normalized interfaces for the VPNs are added to the normalized interface list.

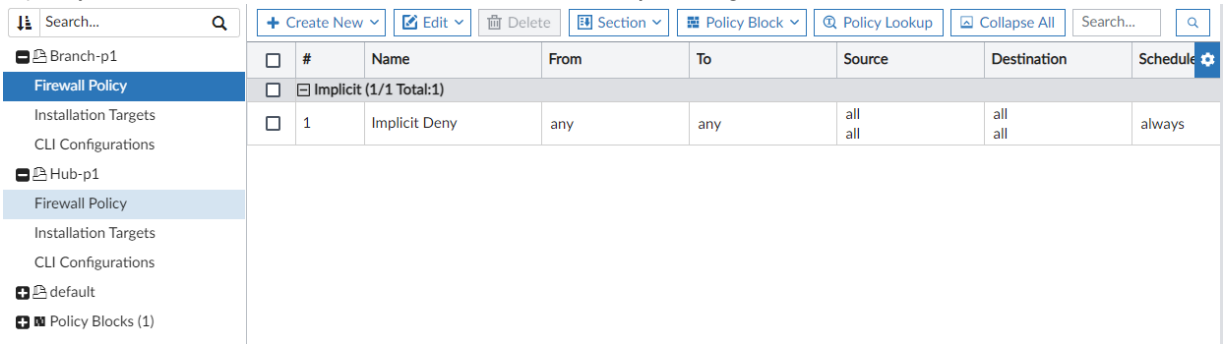
2. **Add Health Check Firewall Policy to Hub/Branch Policy Package**
   Enable the *Add Health Check Firewall Policy to Hub/Branch Policy Package* option to create health check firewall policies (or policy blocks) for HUB(s) and branches.
   - Users must select the HUB and branch policy package that will be used during the wizard configuration. You can select an existing policy package or create a new one.



- Based on the selection, firewall policies (or policy blocks) are created to allow SLA health checks to each device loopback.
- The SD-WAN overlay template creates the policy block and applies it to the top of the HUB Policy Package.



- A policy block is not created for the SD-WAN branch Policy Package.



Automated SD-WAN overlay process adds "branch_id" meta variable auto assignment

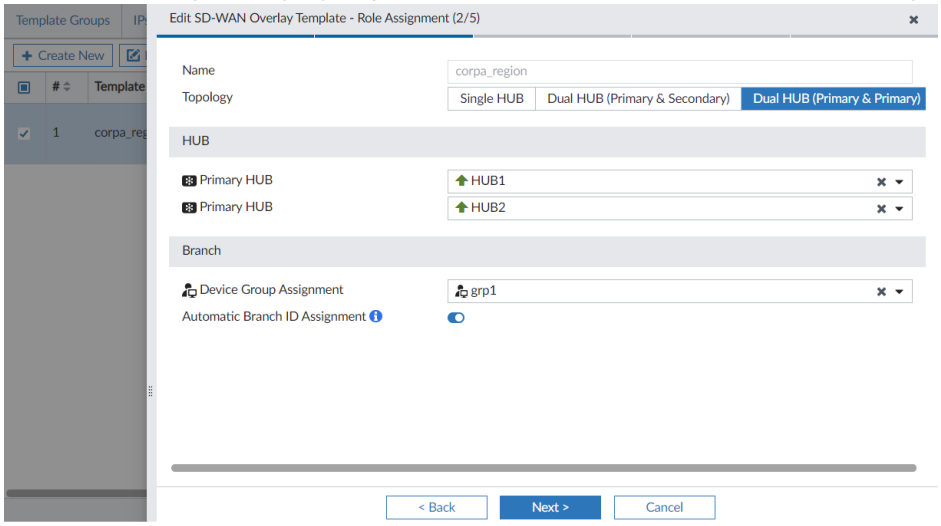
This information is also available in the FortiManager 7.4 Administration Guide:

- Configuring an SD-WAN overlay template
- Objects and templates created by the SD-WAN overlay template

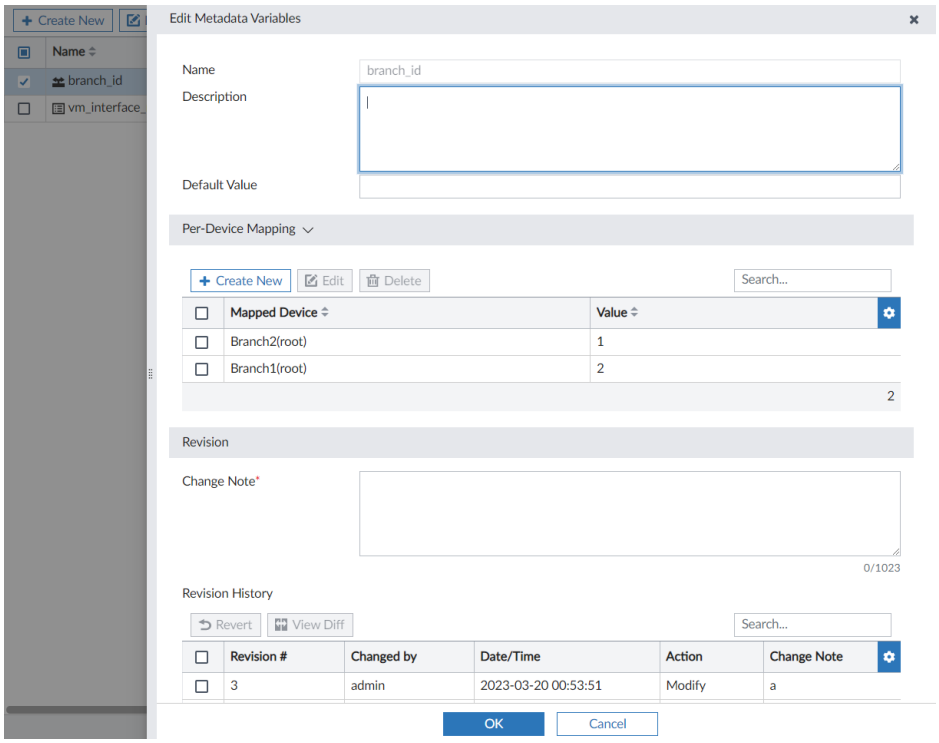
The automated SD-WAN overlay process adds "branch_id" meta variable auto assignment.

To automatically assign branch IDs using the SD-WAN overlay template:

1. Go to *Device Manager* > *Provisioning Templates* > *SD-WAN Overlay Template*.
2. Create or edit an SD-WAN overlay template.
3. On the *Role Assignment (2/5)* step in the wizard, enable *Automatic Branch ID Assignment*.



- When *Automatic Branch ID Assignment* is enabled, FortiManager automatically assigns and tracks a branch ID for each device in the branch device group. This also applies to devices added to the branch device group in the future, as well as those added to the device group using a zero-touch provisioning device blueprint.



- Branch ID values are between one and the maximum number allowed by the subnet. For example, the default 10.10.0.0/255.255.0.0 overlay network uses the /19 subnet when your setup includes 5 - 8 overlays. The maximum allowed branch IDs in this range is 8,190 based on the maximum number of number of usable IPs/FortiGates supported per overlay.

SD-WAN monitoring map integrates with Cloud Assisted Monitoring Service to allow FortiGate interface speed tests from inside FortiManager

This information is also available in the FortiManager7.4 Administration Guide:

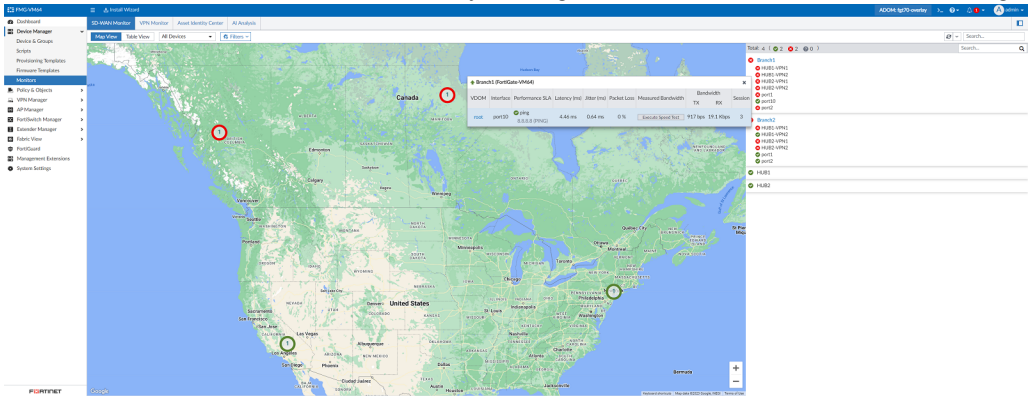
- SD-WAN Cloud assisted monitoring speed test.

SD-WAN Monitoring Map integrates with Cloud Assisted Monitoring Service to allow FortiGate interface speed tests from inside FortiManager.

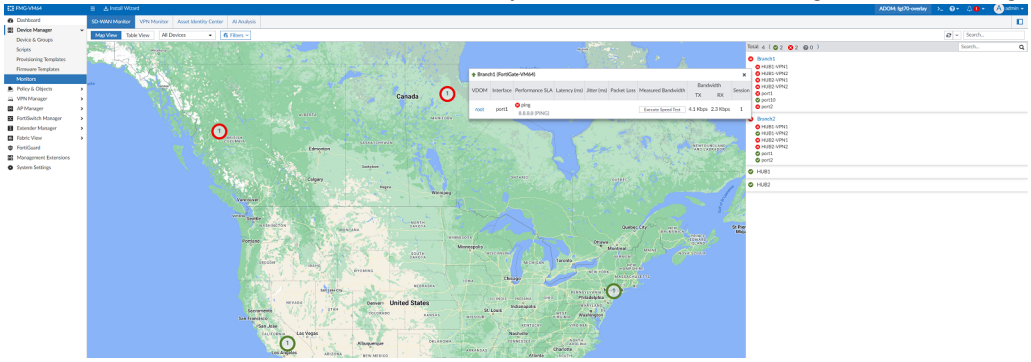
To execute an SD-WAN speed test:

1. Execution of speed tests can be performed from the *SD-WAN Monitor* page: Map View, Table View, Device Drilldown and the Device Dashboard.
2. For devices with a valid license and an interface set with the WAN role, the *Execute Speed Test* option is displayed for the interface.

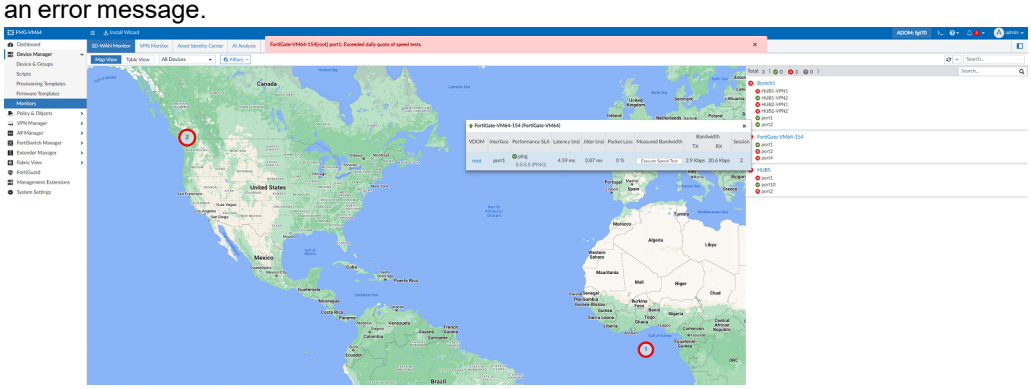
- If there is a valid route to the cloud server, you will get measured bandwidth when executing the speed test.



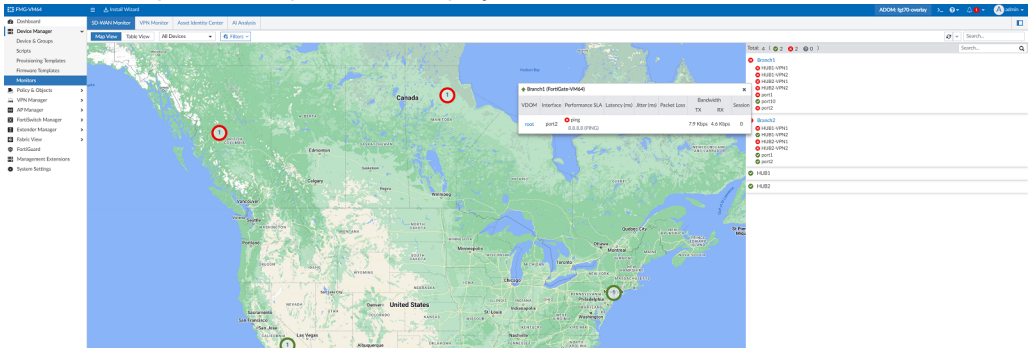
- If there is not a valid route to the cloud server, you will see an error message when executing the speed test.



- You can perform the speed test up to 10 times per day. Attempts to perform additional speed tests will present an error message.



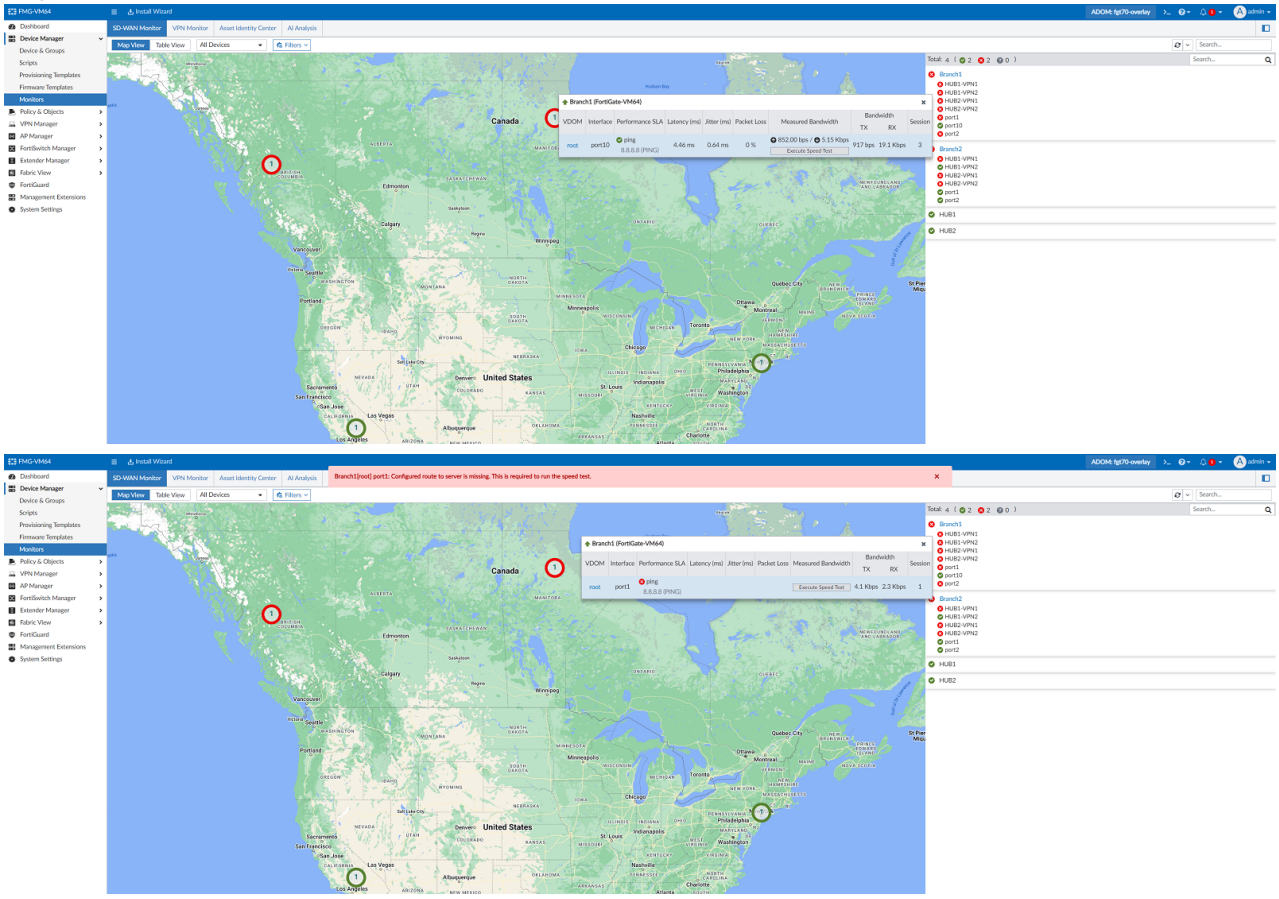
3. For devices without a valid license, or for devices with a valid license but without an interface set to the WAN role, the *Execute Speed Test* option is not displayed.



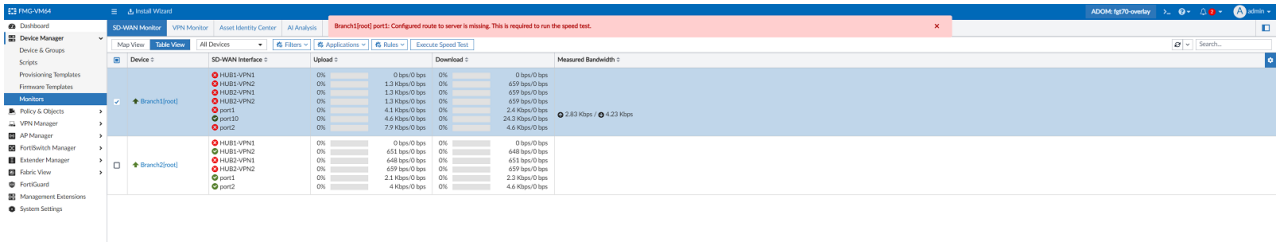
To view the results in SD-WAN Monitor pages:

The latest results of the speed test are displayed on the SD-WAN Monitor pages, including:

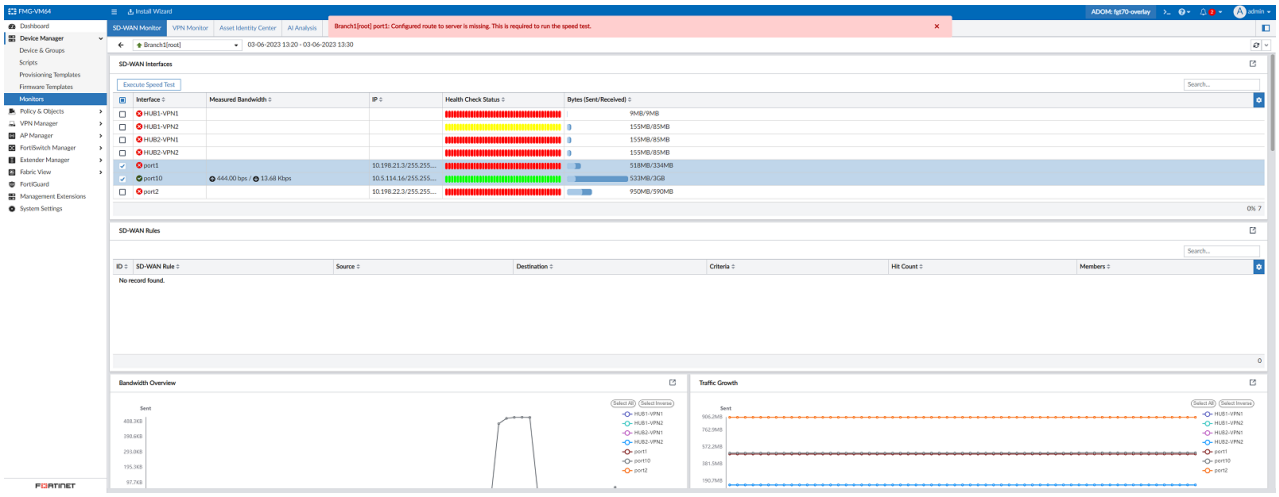
- Map View:



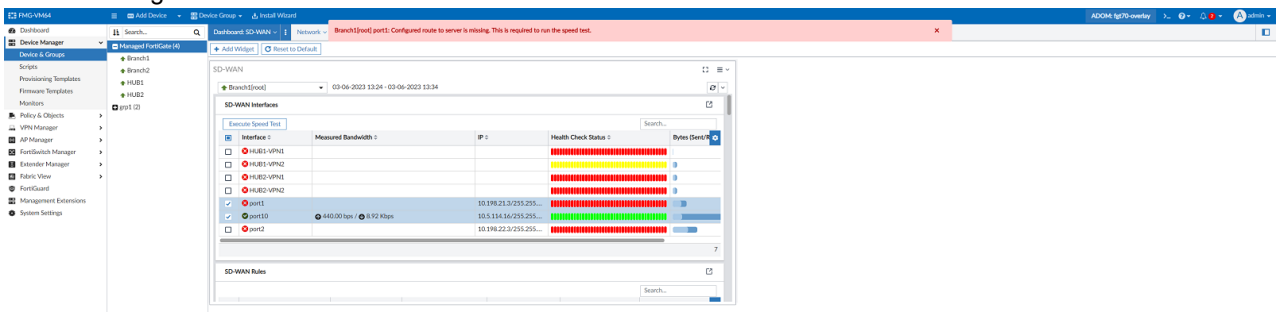
- Table View:



- Device Drilldown:



- Device Manager > Device Dashboard > SD-WAN Monitor:



SDWAN monitoring map enhancements

This information is also available in the FortiManager 7.4 Administration Guide:

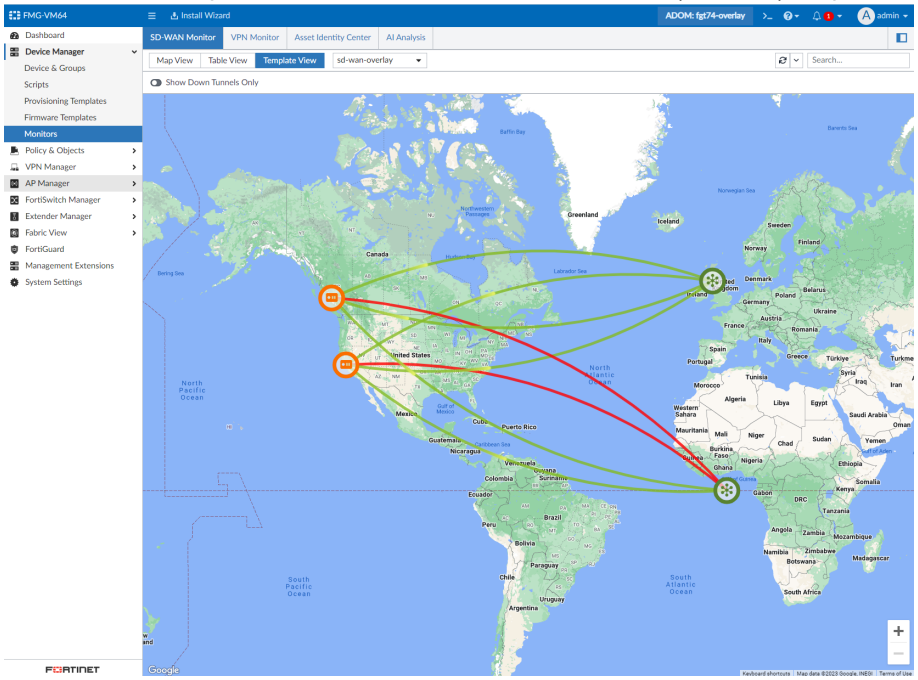
- Template View

SDWAN monitoring map differentiates HUB and branch device types, displays the overlay connectivity between devices and WAN underlay ports SLA performances.

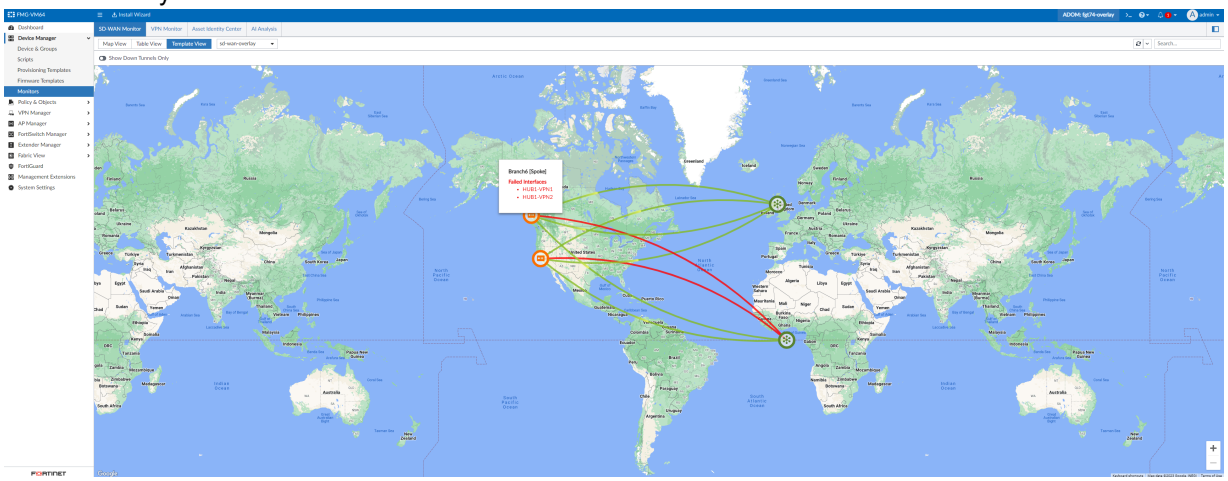
To monitor SD-WAN with the Template View:

1. Go to the *Device Manager* > *Monitors* > *SD-WAN Monitor* pane, and click *Template View*.
   - SD-WAN devices provisioned using the currently selected SD-WAN template are displayed on the map.
   - Only devices provisioned using the selected SD-WAN template are displayed. You can change the selected SD-WAN template by clicking the dropdown in the toolbar and selecting a new template.

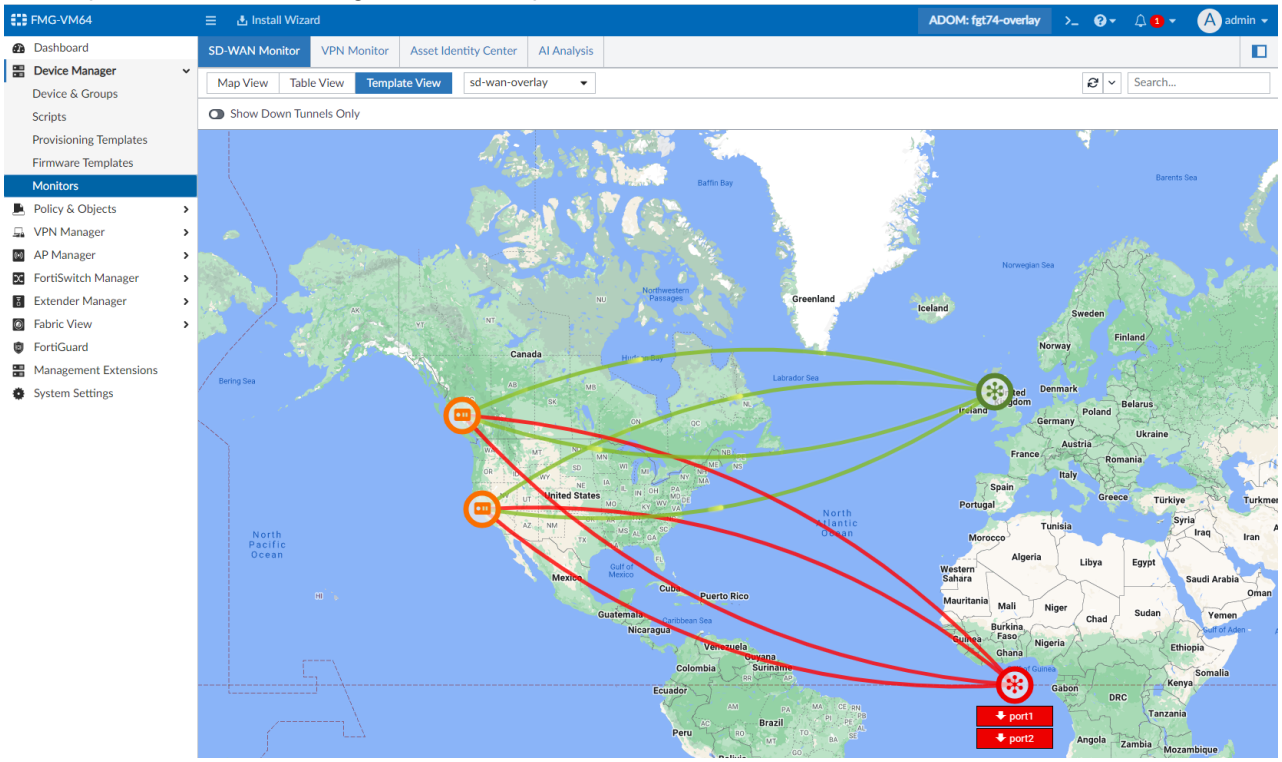
- Devices on the map are identified with icons as either a HUB (star icon) or spoke device (device icon).



2. Hovering your mouse over a device on the map displays the following information:
   - Device name and whether it is a HUB or spoke.
   - Interfaces that have a failed health check.
   - Down underlays.



3. The map shows lines connecting the HUB and spoke devices.



The line color depends on if the tunnel is up (green) or down (red). Device color is based off of the following logic:

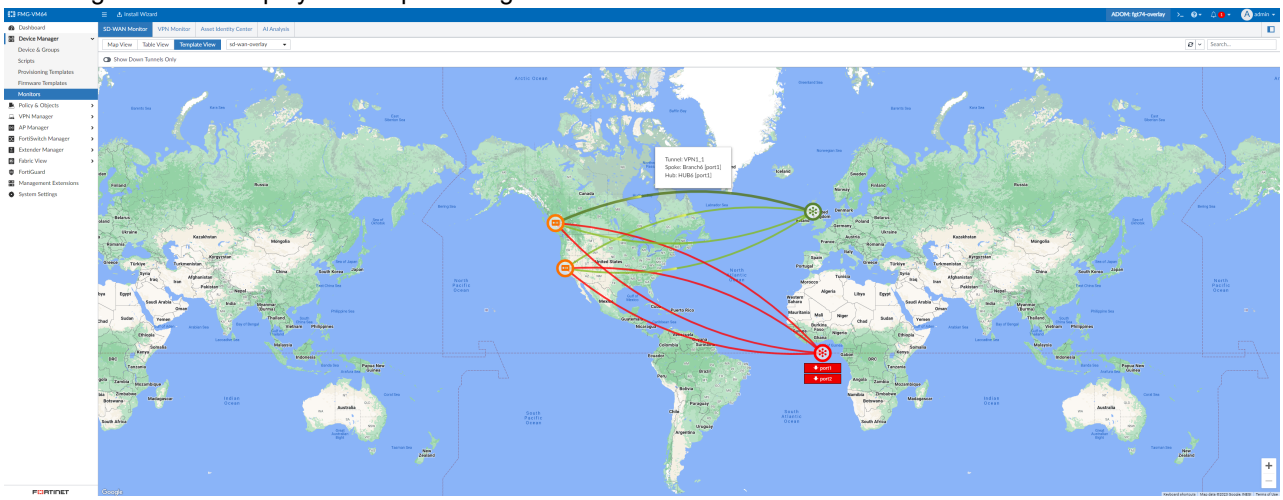
a. If the SD-WAN health checks are defined on the device (usually a spoke):

- Green: All health checks pass.
- Orange: Some health checks pass.
- Red: All health checks fail.

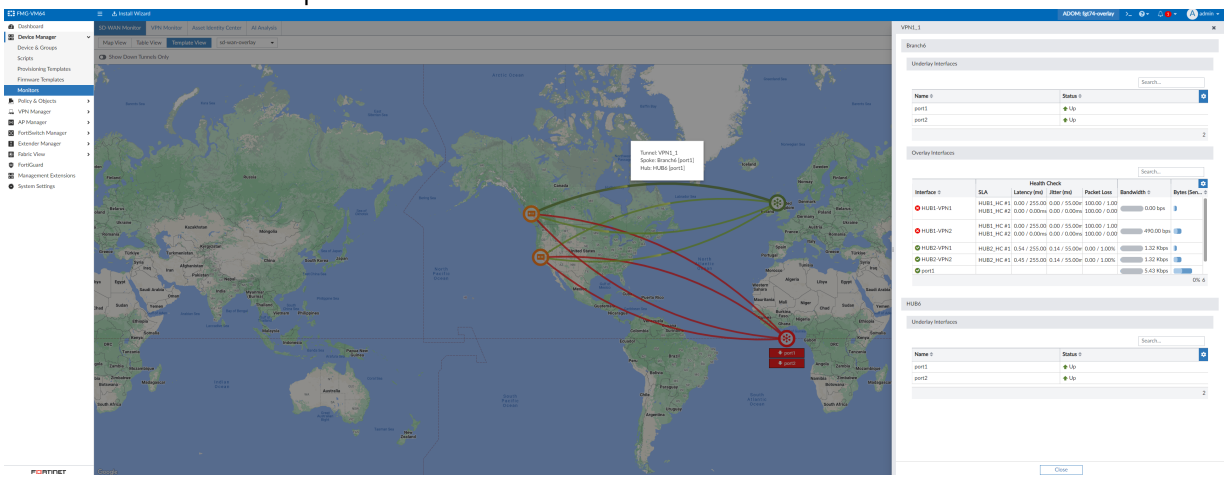
b. When no SD-WAN health checks are defined on the device (usually a HUB):

- Green: All underlays are up.
- Orange: Some underlays are up.
- Red: All underlays are down.

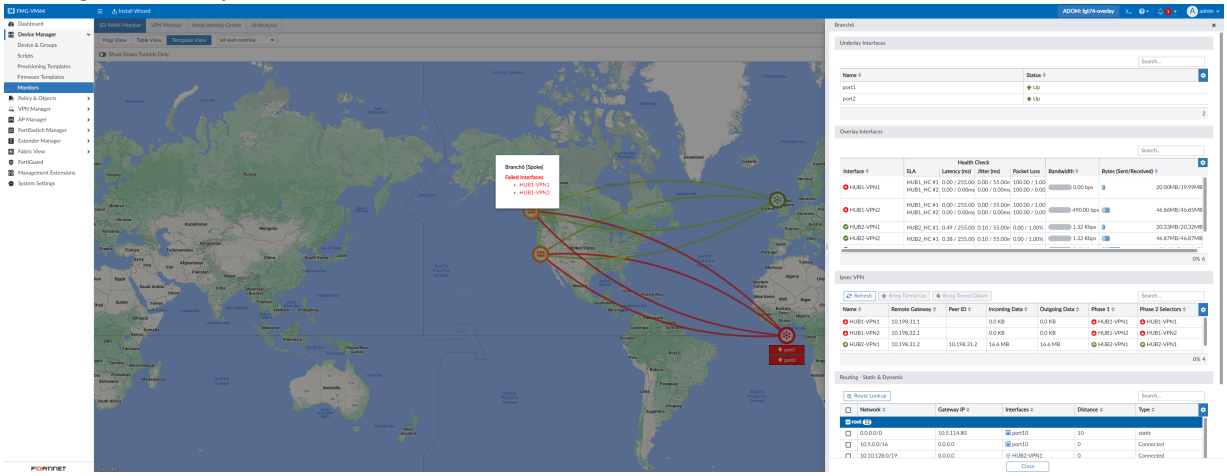
4. Hovering over a line displays a tooltip showing both device names.



5. Clicking on a line opens a pane with the following information:
   - Underlay Status table of HUB and spoke devices.
   - Health check table for the spoke devices.

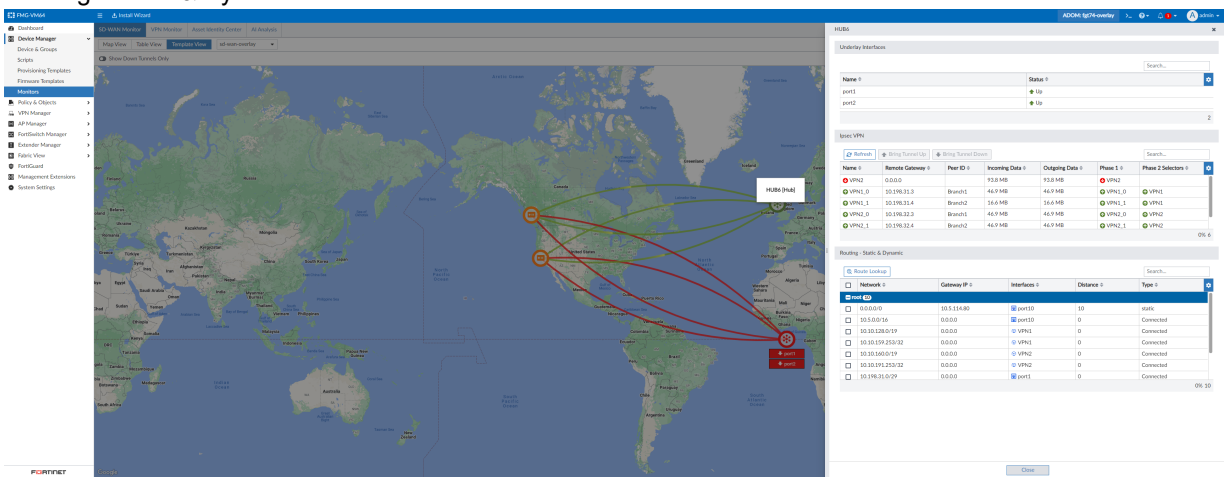


6. Clicking on a spoke device opens a pane with the following information.
   - SD-WAN health check table.
   - Underlay status table.
   - IPsec VPN table.
   - Routing - Static & Dynamic table.



7. Clicking on a HUB device opens a pane with the following information:
   - Underlay Status table.
   - IPsec VPN table.

- Routing - Static & Dynamic table.



SDWAN template for heterogeneous WAN link types

This information is also available in the FortiManager 7.4 Administration Guide:

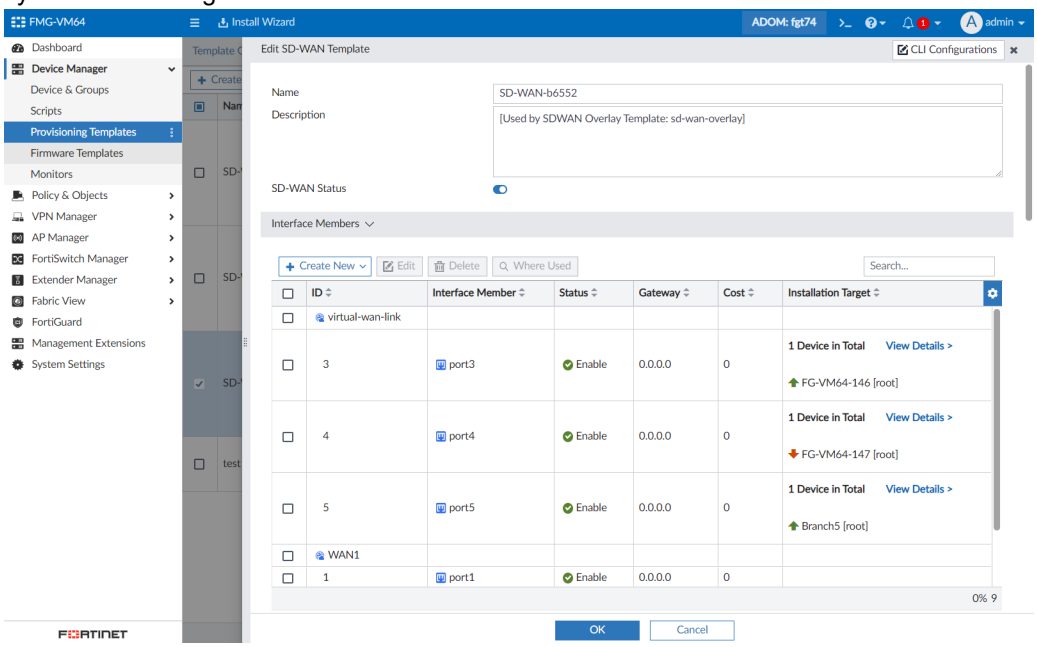
- Zones and interface members
- Performance SLA

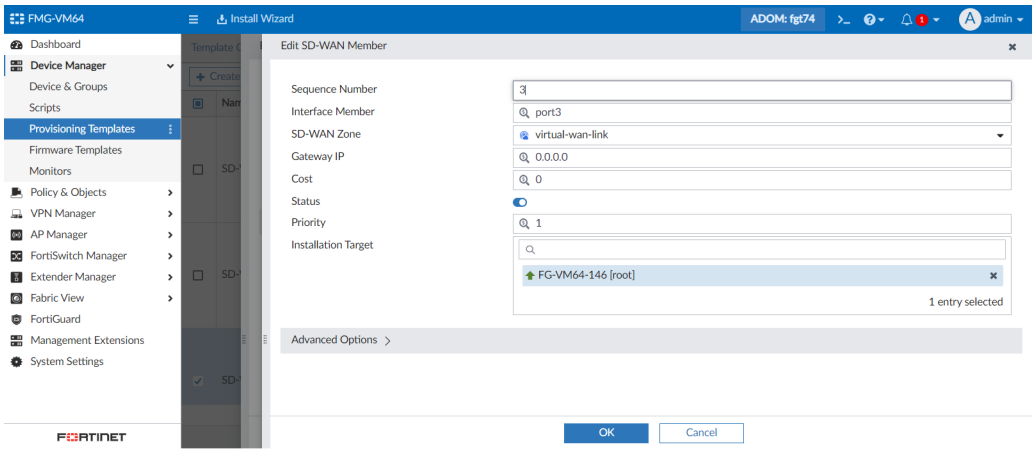
SDWAN template for heterogeneous WAN link types to support single-template usage for FortiGates with different underlay connections and SLAs.

To create an SD-WAN template with heterogeneous WAN links:

1. Go to *Device Manager* > *Provisioning Templates* > *SD-WAN Template*, and create or edit a template.
2. You can select the installation target for the following SD-WAN objects:
   - system sdwan members
   - system sdwan service
   - system sdwan health-check

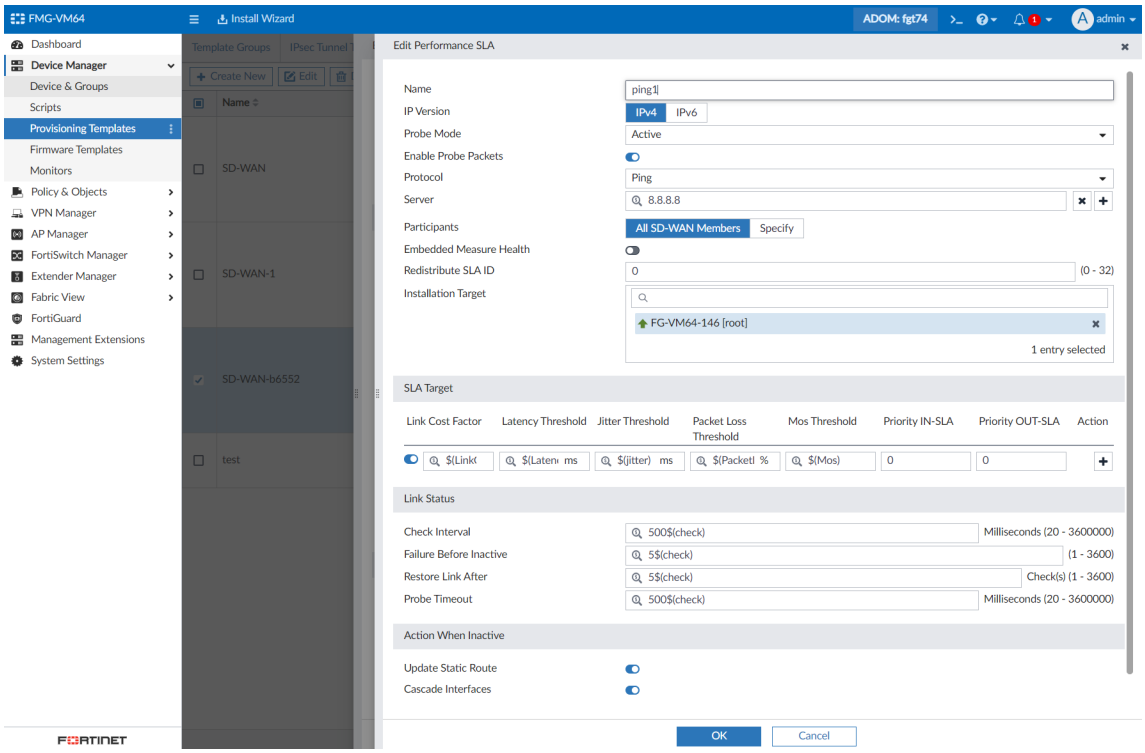
- system sdwan neighbor





3. You can add meta variables for the following health-check attributes:
   - System SD-WAN health-check
     - Check Interval
     - Fail Before Inactive
     - Probe Timeout
     - Restore Link After
   - System SD-WAN health-check SLA
     - Link Cost Factor
     - Latency Threshold
     - Jitter Threshold
     - Packet Loss Threshold

- Mos Threshold



Templates

This section lists the new features added to FortiManager for templates:

- Preview CLI configuration for the device provisioning templates on page 25
- Fortinet factory-default wireless and extender templates on page 28
- Jinja Templates have direct access to the device DB to support generation of dynamic configuration on page 34
- Fabric Authorization Template is integrated with Device Blueprint and supports meta variables 7.4.1 on page 41

Preview CLI configuration for the device provisioning templates

This information is also available in the FortiManager 7.4 Administration Guide:

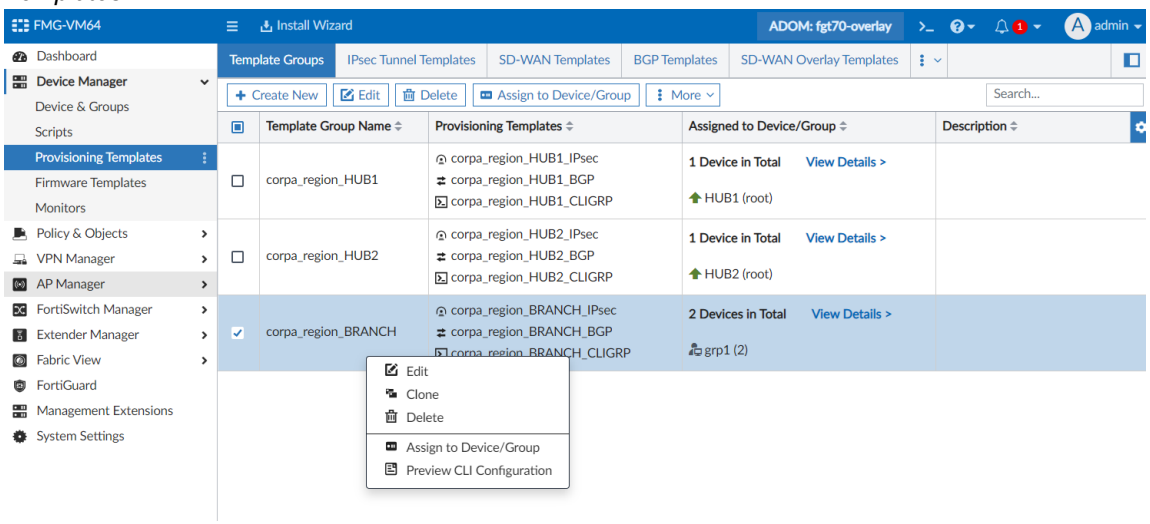
- Viewing the CLI preview for provisioning templates

In FortiManager, you can preview the CLI configuration for the device provisioning templates.

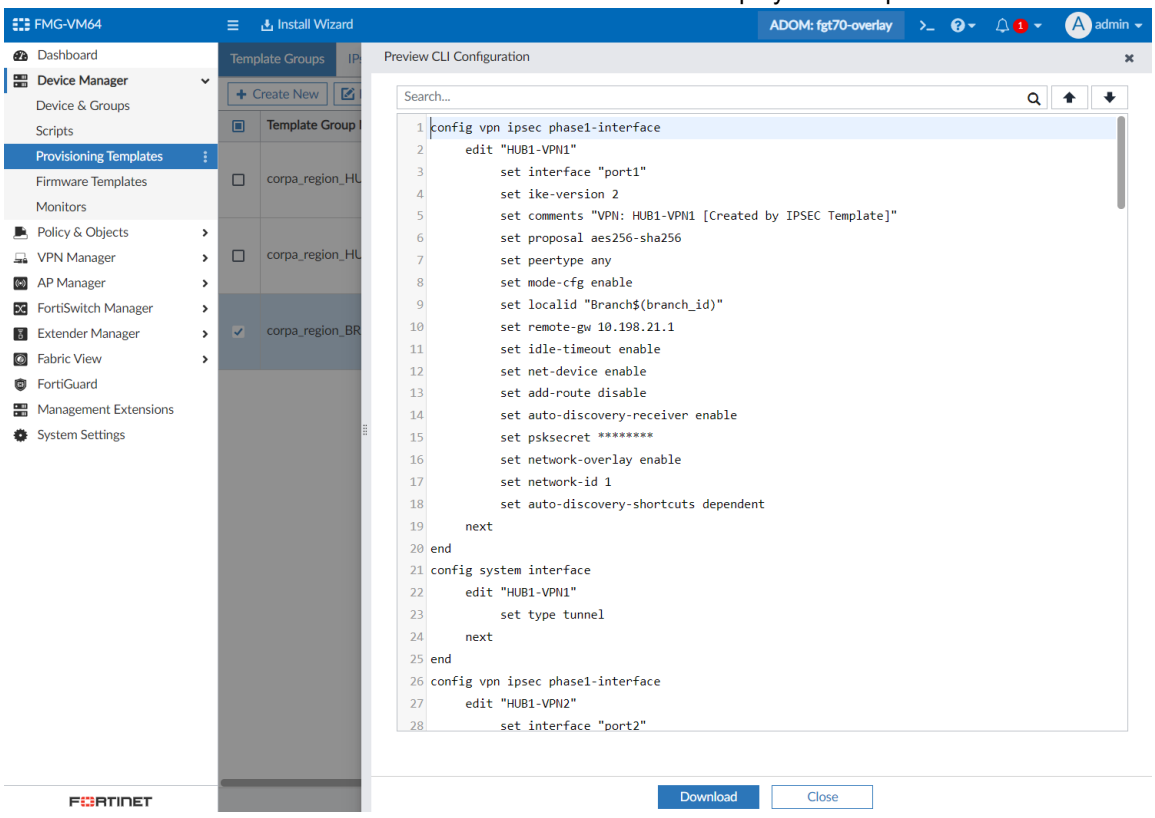
To preview the CLI configuration for provisioning templates:

1. Go to *Device Manager* > *Provisioning Templates*.
   Select a template type by choosing the corresponding tab. You can view the CLI preview for all provisioning template types, including: *Template Groups*, *IPsec Tunnel Templates*, *SD-WAN Templates*, *BGP Templates*, *SD-*

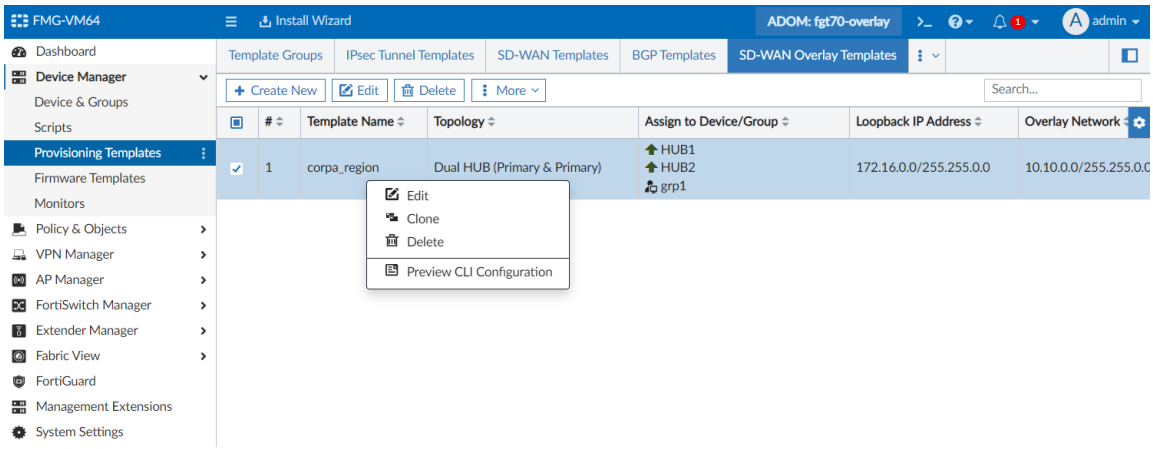
WAN Overlay Templates, *System Templates*, *Static Route Templates*, *CLI Templates*, and *Threat Weight Templates*.

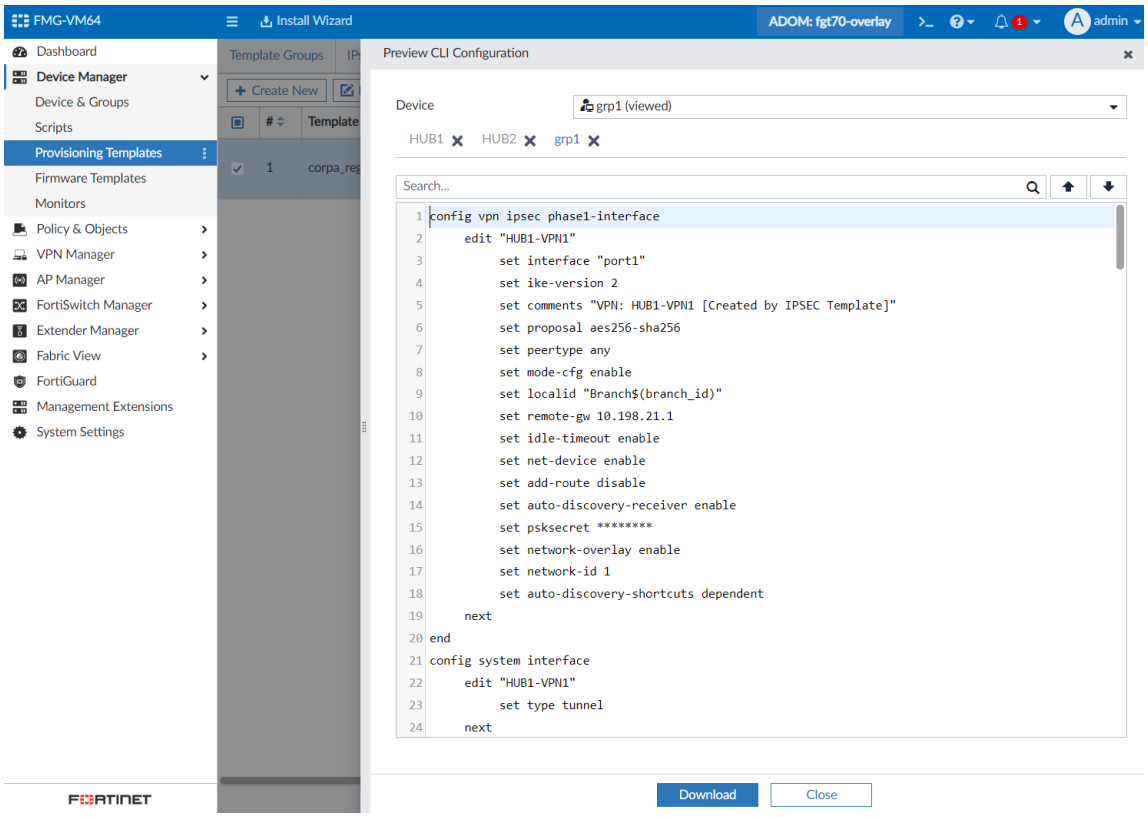


2. Right-click on a template, and choose *Preview CLI Configuration*.
The *Preview CLI Configuration* window is displayed with the CLI configuration for the selected template. The metadata variable names and not their resolved values are displayed in the preview.

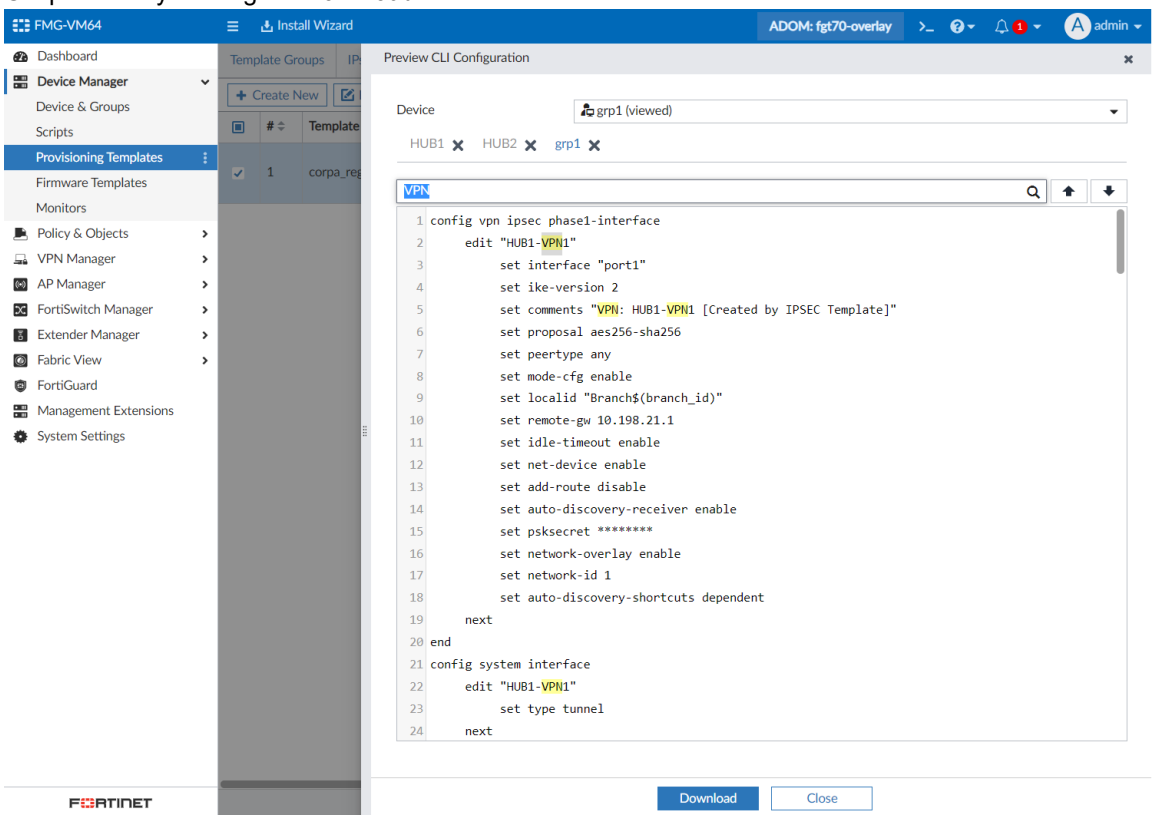


3. When the provisioning template includes multiple devices, you can select a device from the *Device* dropdown. The CLI preview for the selected device is displayed in the content pane.


FMG-VM64
Install Wizard
ADOM: fgt70-overlay
admin
Dashboard
Device Manager
Device & Groups
Scripts
Provisioning Templates
Firmware Templates
Monitors
Policy & Objects
VPN Manager
AP Manager
FortiSwitch Manager
Extender Manager
Fabric View
FortiGuard
Management Extensions
System Settings
Template Groups
IPsec Tunnel Templates
SD-WAN Templates
BGP Templates
SD-WAN Overlay Templates
Create New
Edit
Delete
More
Search...
Template Name Topology Assign to Device/Group Loopback IP Address Overlay Network
1 corpa_region Dual HUB (Primary & Primary) HUB1 HUB2 grp1 172.16.0.0/255.255.0.0 10.10.0.0/255.255.0.0
Edit
Clone
Delete
Preview CLI Configuration


FMG-VM64
Install Wizard
ADOM: fgt70-overlay
admin
Dashboard
Device Manager
Device & Groups
Scripts
Provisioning Templates
Firmware Templates
Monitors
Policy & Objects
VPN Manager
AP Manager
FortiSwitch Manager
Extender Manager
Fabric View
FortiGuard
Management Extensions
System Settings
Preview CLI Configuration
Device
grp1 (viewed)
HUB1
HUB2
grp1
Search...
config vpn ipsec phase1-interface
edit "HUB1-VPN1"
set interface "port1"
set ike-version 2
set comments "VPN: HUB1-VPN1 [Created by IPSEC Template]"
set proposal aes256-sha256
set peertype any
set mode-cfg enable
set localid "Branch$(branch_id)"
set remote-gw 10.198.21.1
set idle-timeout enable
set net-device enable
set add-route disable
set auto-discovery-receiver enable
set psksecret ********
set network-overlay enable
set network-id 1
set auto-discovery-shortcuts dependent
next
end
config system interface
edit "HUB1-VPN1"
set type tunnel
next
Download
Close

4. In the *Preview CLI Configuration* window, you can search in the CLI using the search bar, and you can download the CLI preview by clicking the *Download* button.



Fortinet factory-default wireless and extender templates

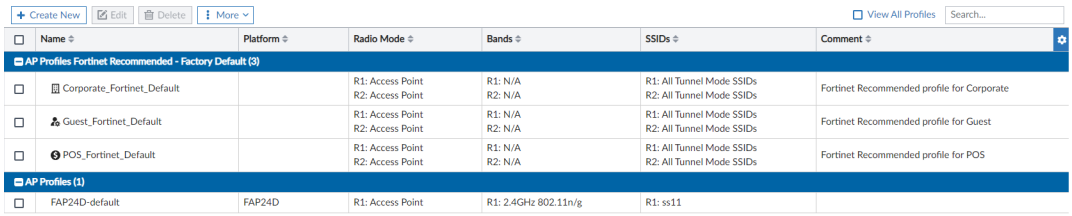
FortiManager includes Fortinet factory-default wireless and extender templates with built-in security and network configuration based on best security practices.

This information is also available in the FortiManager 7.4 Administration Guide:

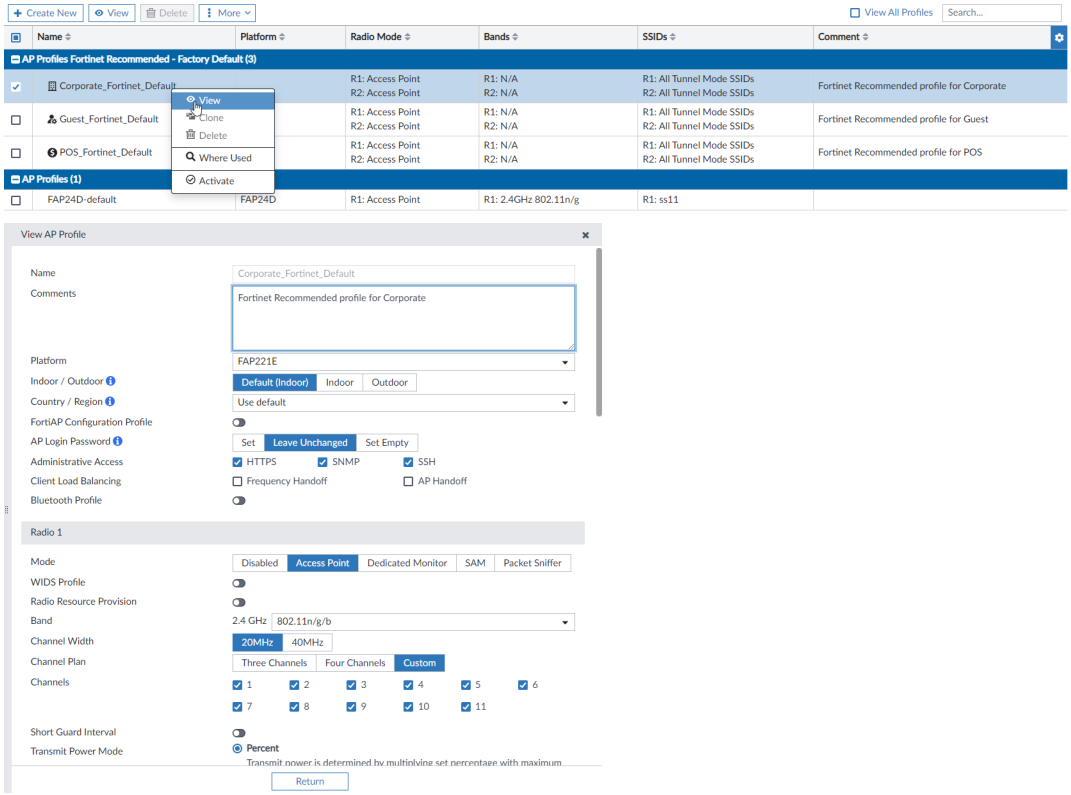
- Using Fortinet recommended FortiAP and SSID profiles
- Using Fortinet recommended extender profiles

To use default FortiAP profiles and SSIDs:

1. Recommended FortiAP profiles are available in the FortiManager *AP Manager*.
   a. Go to *AP Manager* > *Operation Profiles* under the *FortiAP Profiles* tab.

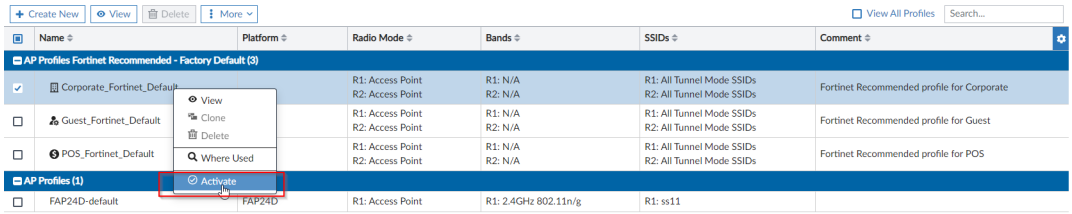


b. Right click on a recommended AP profile and click *View*.

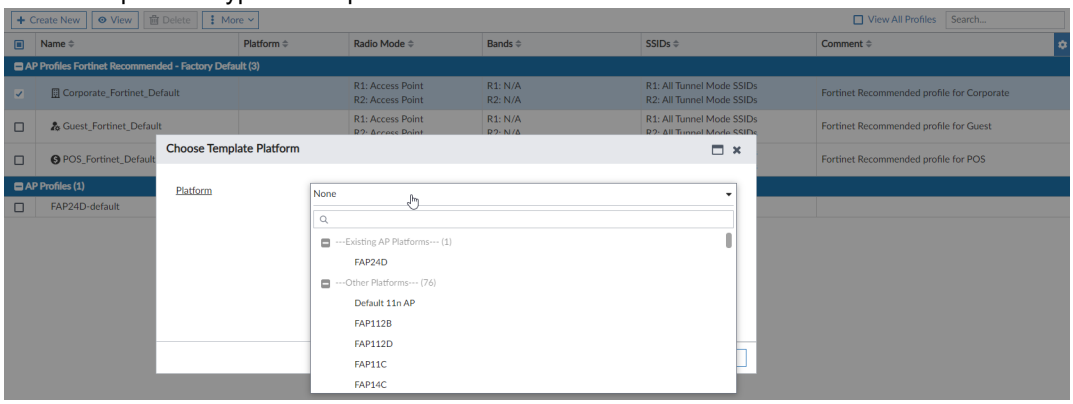


2. FortiAP profiles based on the recommended profiles can be created by activating the recommended profiles.

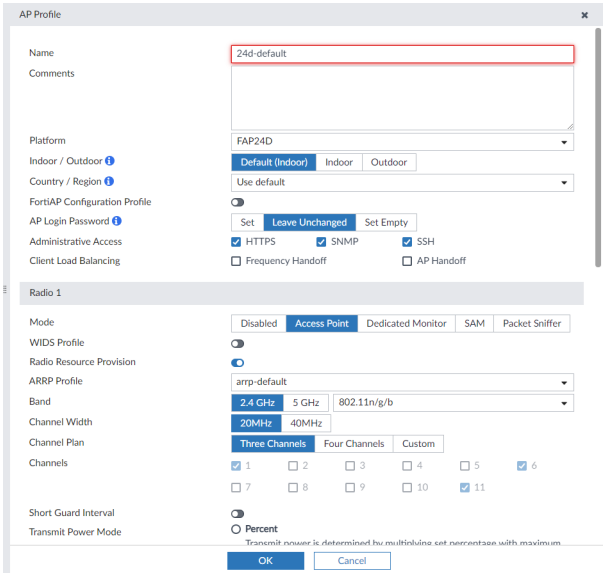
a. Right-click on a recommended profile and click *Activate*.



b. Select the platform type for the profile.

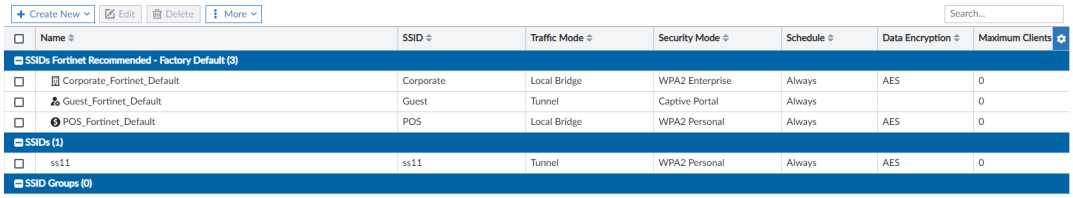


c. Enter a name for the AP profile and configure the remaining settings if required.

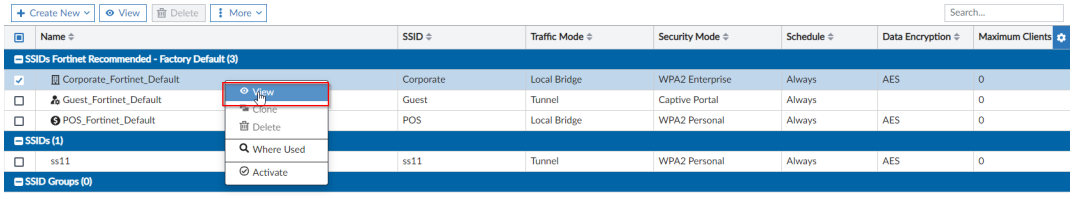


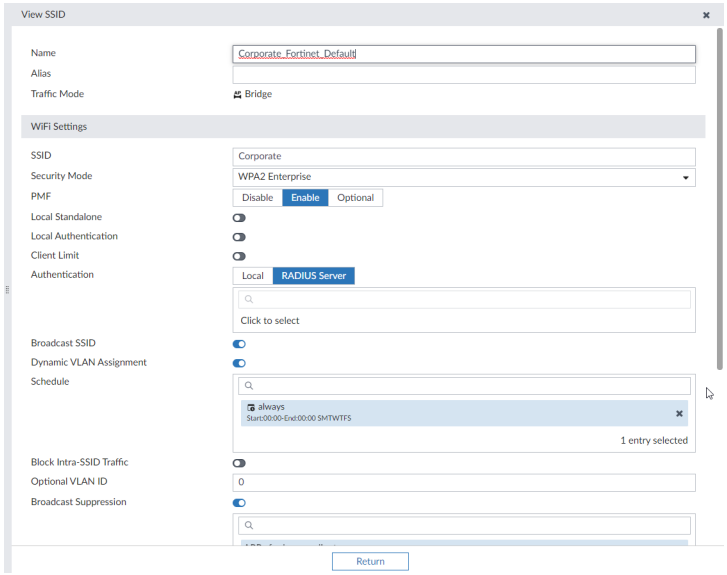
3. The recommended default AP SSIDs are shown in *AP Manager* > *SSIDs*.

a. Go to *FortiAP* > *SSIDs* to view the default SSIDs.



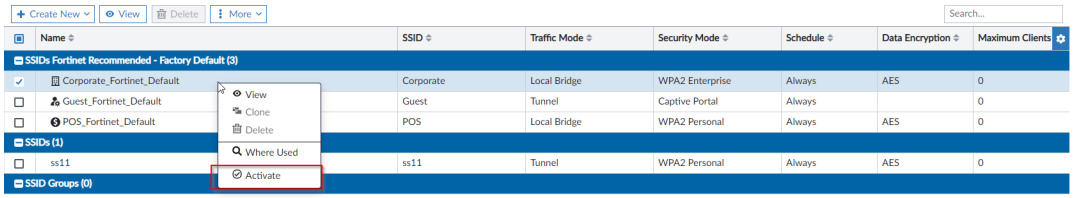
b. Right click on a recommended SSID and click *View* to view its details.



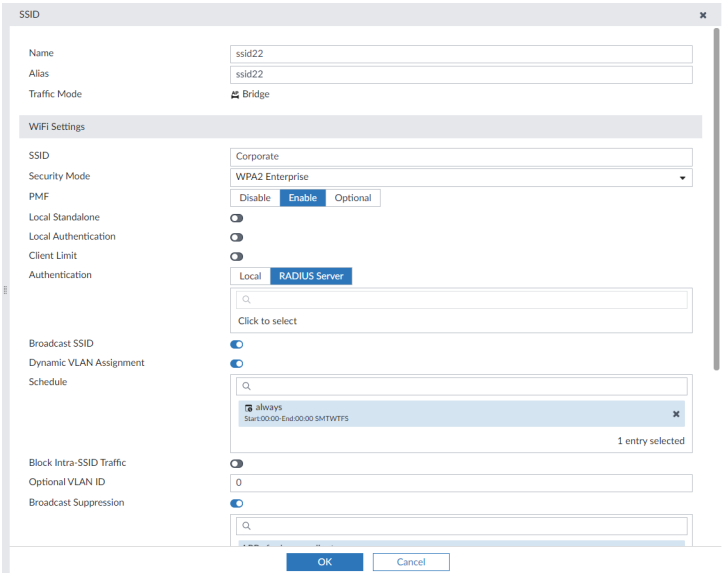


4. An SSID can be created by activating the recommended SSIDs.

a. Right-click on a recommended SSID and click *Activate*.

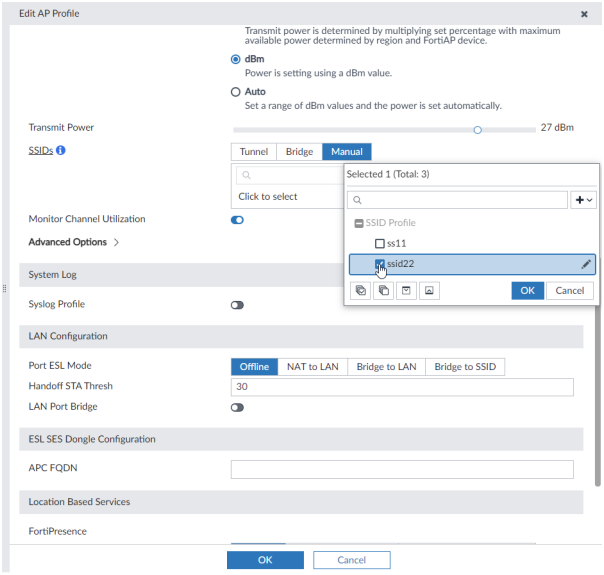


b. Enter a name for the SSID and configure the remaining settings as needed.

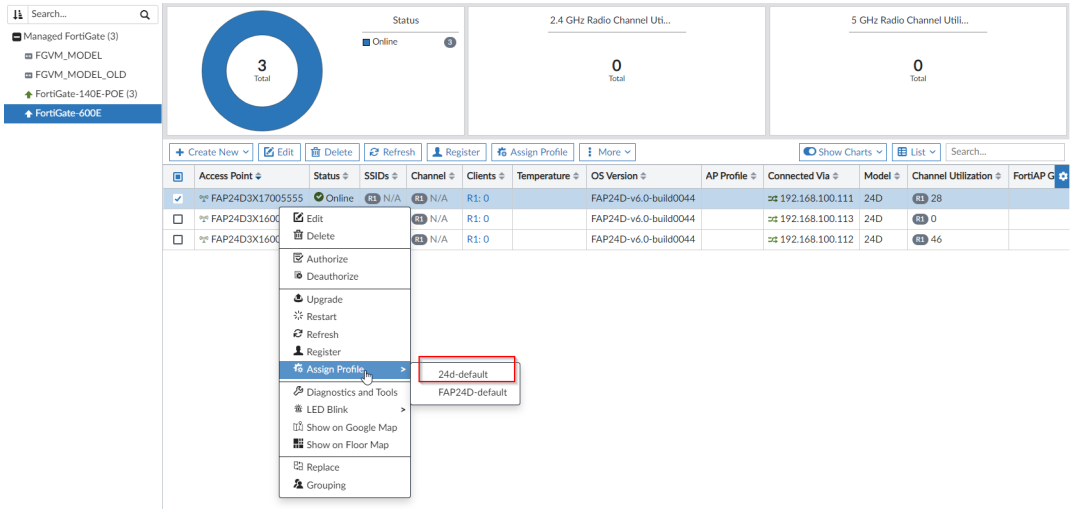


5. The created SSID can be assigned to an AP profile, and the profile can be assigned to the FortiAP.

a. In the FortiAP Profile, select the configured SSID.

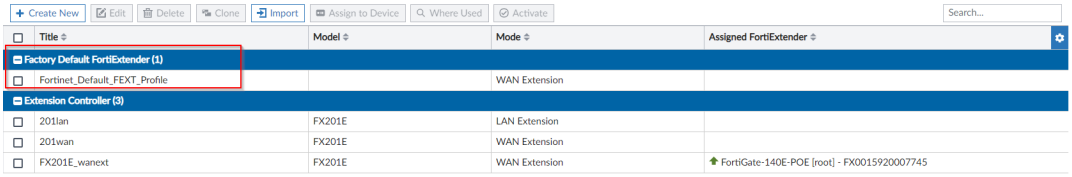


b. Assign the profile to the FortiAP device.

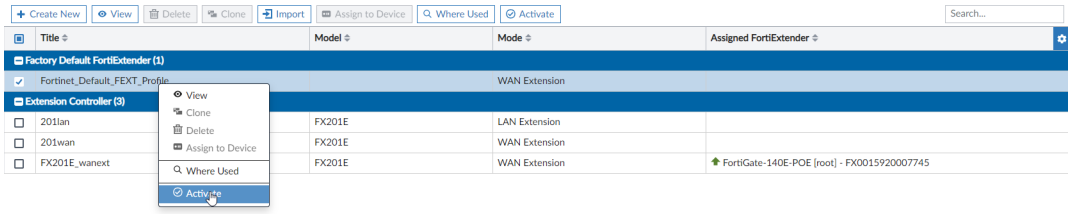


To use recommended FortiExtender templates:

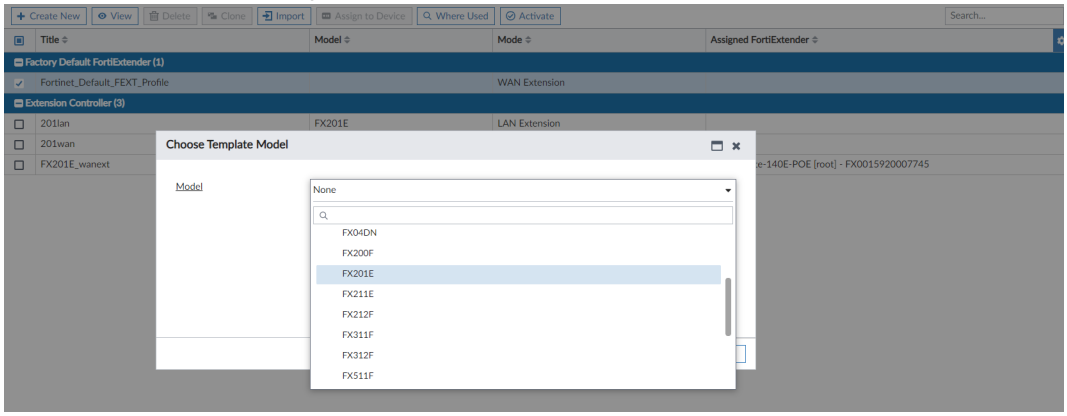
1. The recommended Extender Profile is shown in *Extender Manager* > *Extender Profiles*.



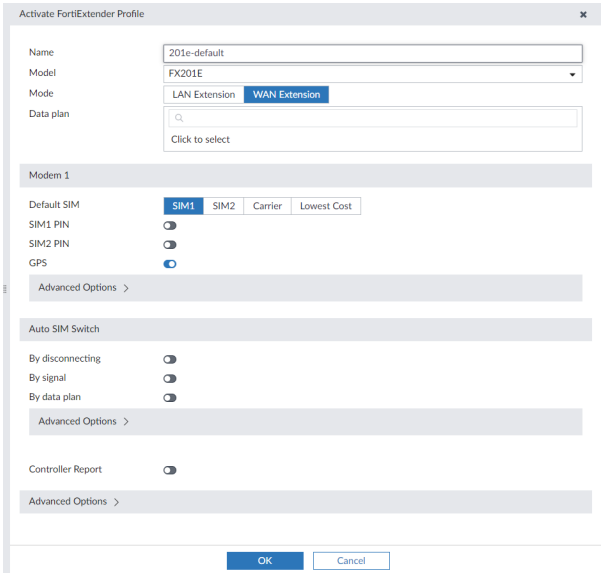
2. An extender profile can be created by activating the recommended FortiExtender profile.
   a. Right-click on the recommended FortiExtender profile and click *Activate*.



   b. Choose a model for the template.

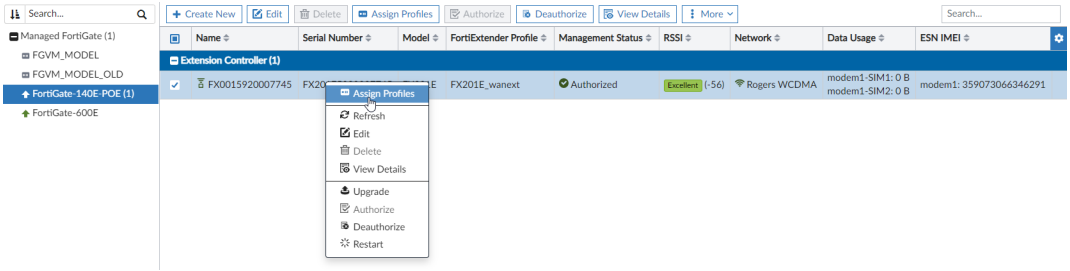


c. Enter a name for the FortiExtender profile and configure the remaining settings as needed.

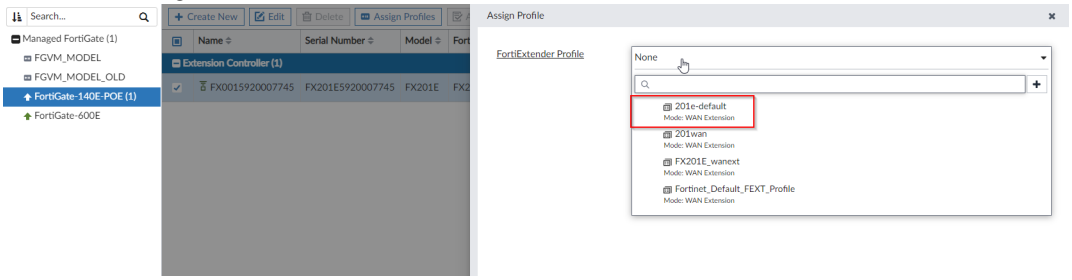


3. The created extender profile can be assigned to an extender, then the user can deploy the settings.

a. Right-click on a managed FortiExtender and click *Assign Profiles*.



b. Select the configured FortiExtender Profile.



Jinja Templates have direct access to the device DB to support generation of dynamic configuration

This information is also available in the FortiManager 7.4 Administration Guide:

- Using FortiManager device database variables in Jinja

Jinja Templates have direct access to the device database to support generation of dynamic configuration.

The following FortiManager variables are supported:

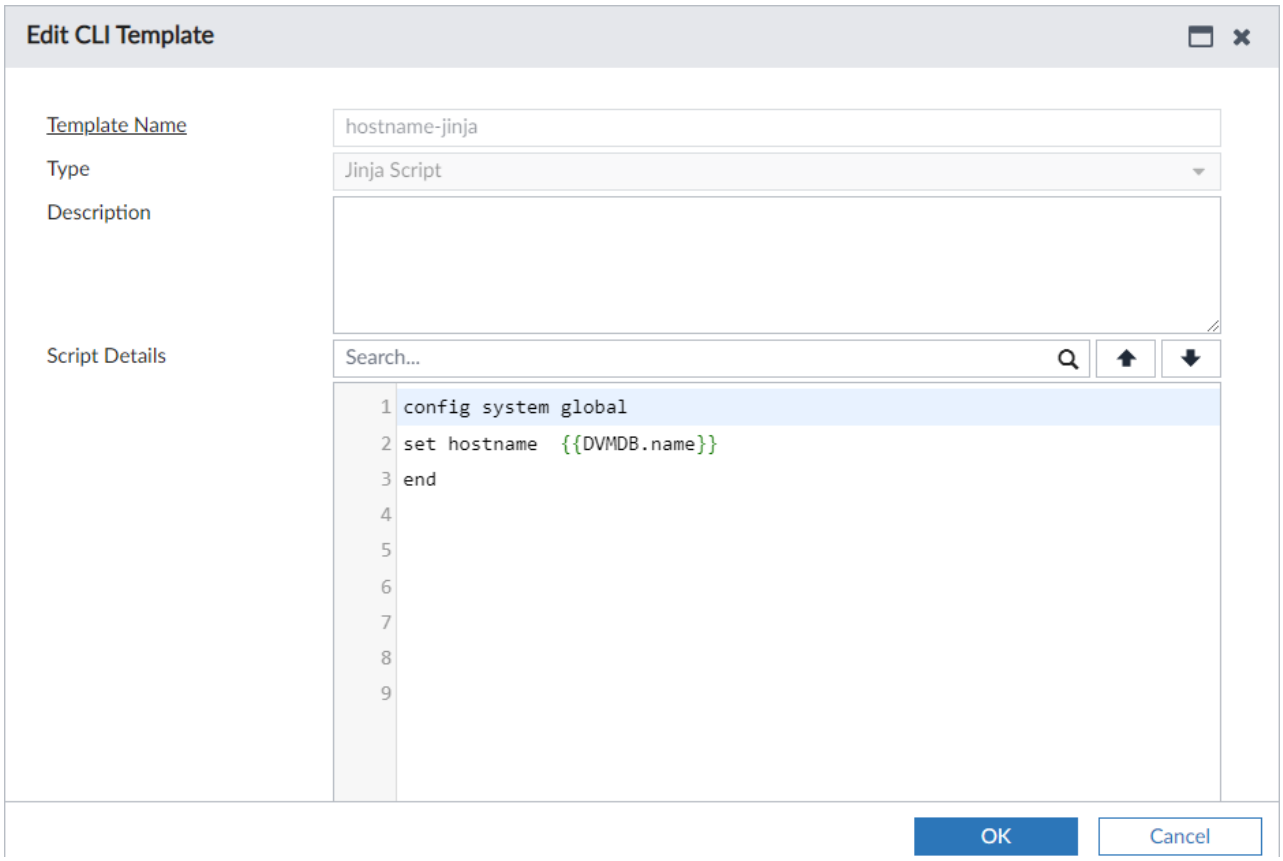
Supported Device Database Variables	Supported System Interface Variables
• **Name**: {{DVMDB.name}} • **Serial**: {{DVMDB.serial}} • **OS TYPE**: {{DVMDB.os_type}} • **Platform**: {{DVMDB.platform}} • **Version**: {{DVMDB.version}} • **Hostname**: {{DVMDB.hostname}} • **UUID**: {{DVMDB.mgmt_uuid}} • **Mgmt Interface IP** : {{DVMDB.mgmt_if}} • **IP**: {{DVMDB.ip}} • **Tunnel IP**: {{DVMDB.tunnel_ip}} • **Description**: {{DVMDB.description}}	• **Interface Name**: {{intf.name}} • **Interface Allowaccess**: {{intf.allowaccess}} • **Interface Type**: {{intf.type}} • **Interface IP**: {{intf.ip}} • **Interface Mode**: {{intf.mode}} • **Interface VDOM**: {{intf.vdom}}

This topic includes the following:

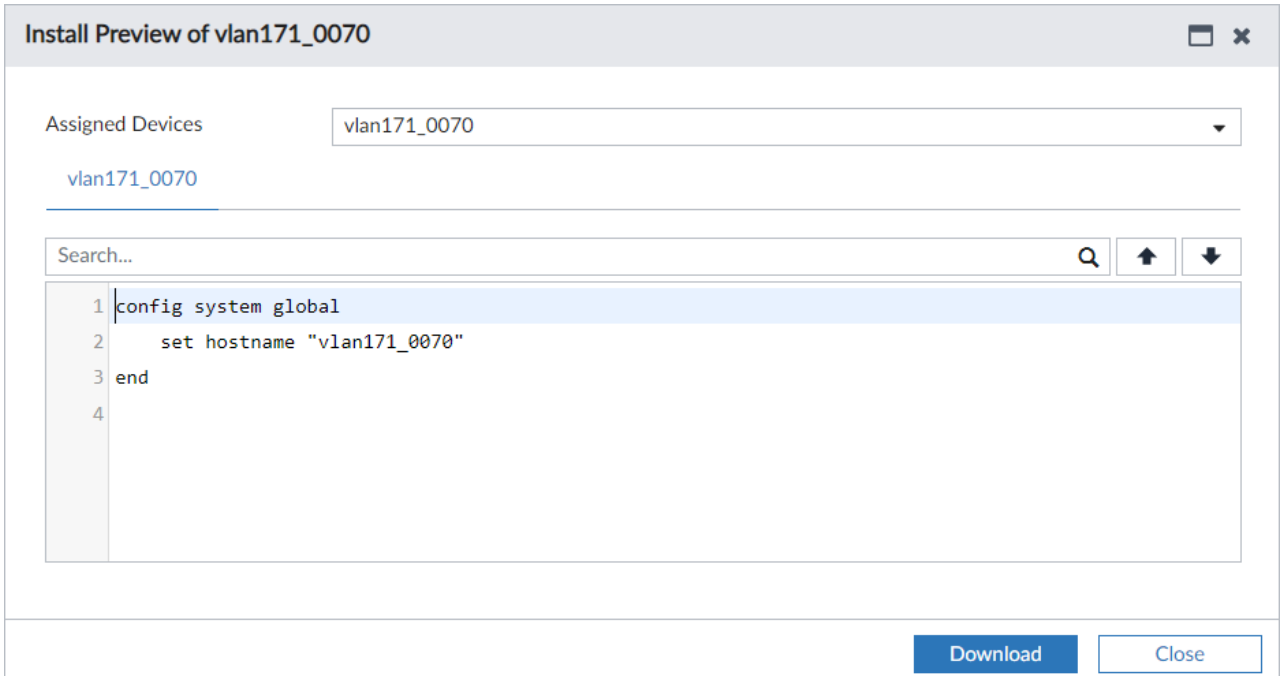
To use device database variables in a Jinja template:

1. Go to *Device Manager* > *Provisioning Templates* > *CLI Template*.
2. Create a new CLI template.
3. Select the *Type* as *Jinja Script*.
4. Configure the *Script Details* with FortiManager variables. For example, you can use *DVMDB.name* as a variable to get the device name from the Device Database:

```
config system global
set hostname {{DVMDB.name}}
end
```



When viewing the *Install Preview* for the CLI Template, the variable *DVMDB.name* is replaced with the *Name* value for the selected device.



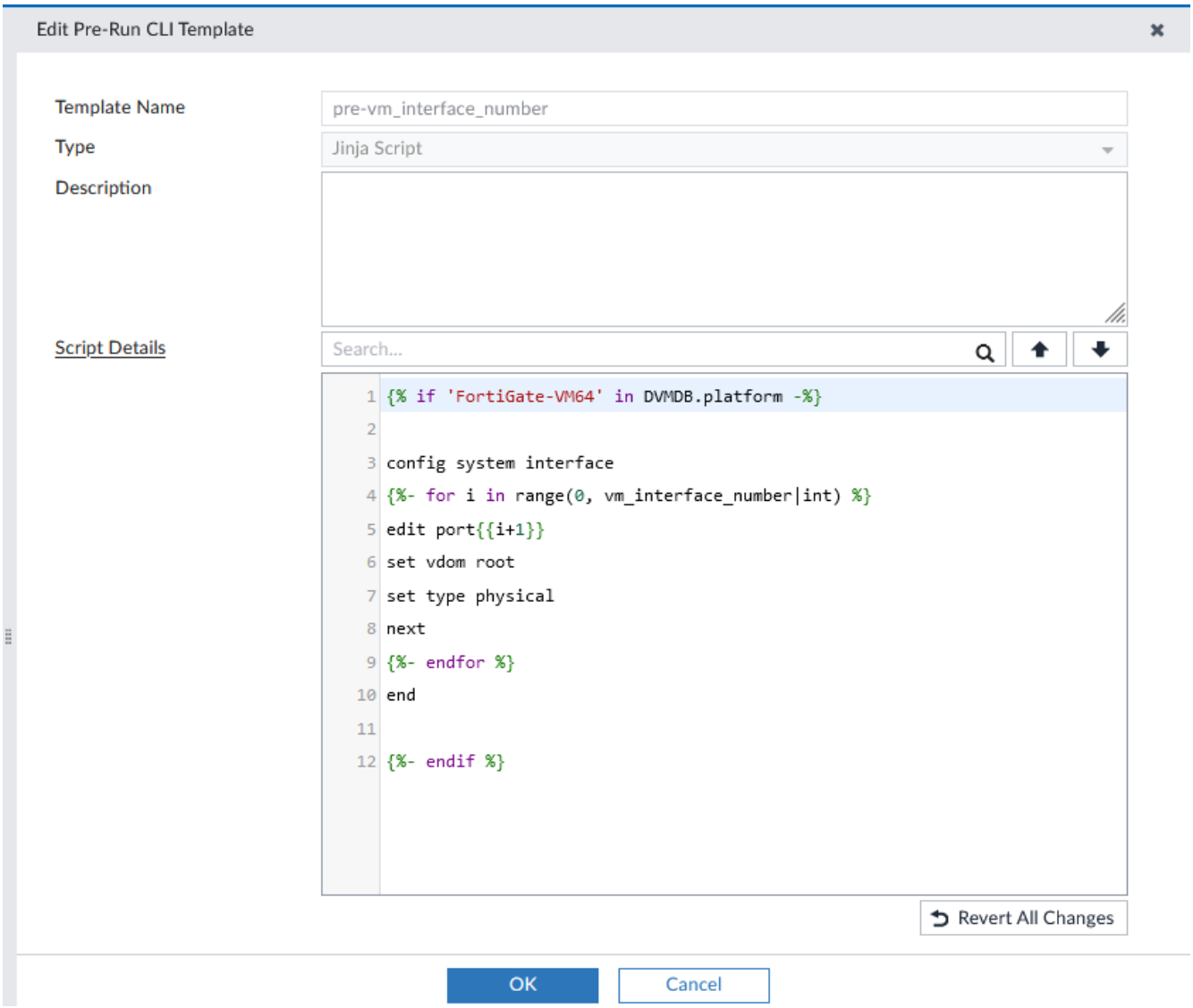
Example 1: Creating physical interfaces for FortiGate-VMs

A user is setting up a FGT-VM64 model device on FortiManager. When setting up a FortiGate-VM, the user needs to execute a script to create the physical interfaces, however, when deploying a FortiGate hardware platform, generating physical interfaces is not necessary. Previously, the user needed to create a separate device group for their FortiGate-VM devices and then runs a script to create the physical interfaces for VM devices inside the device group.

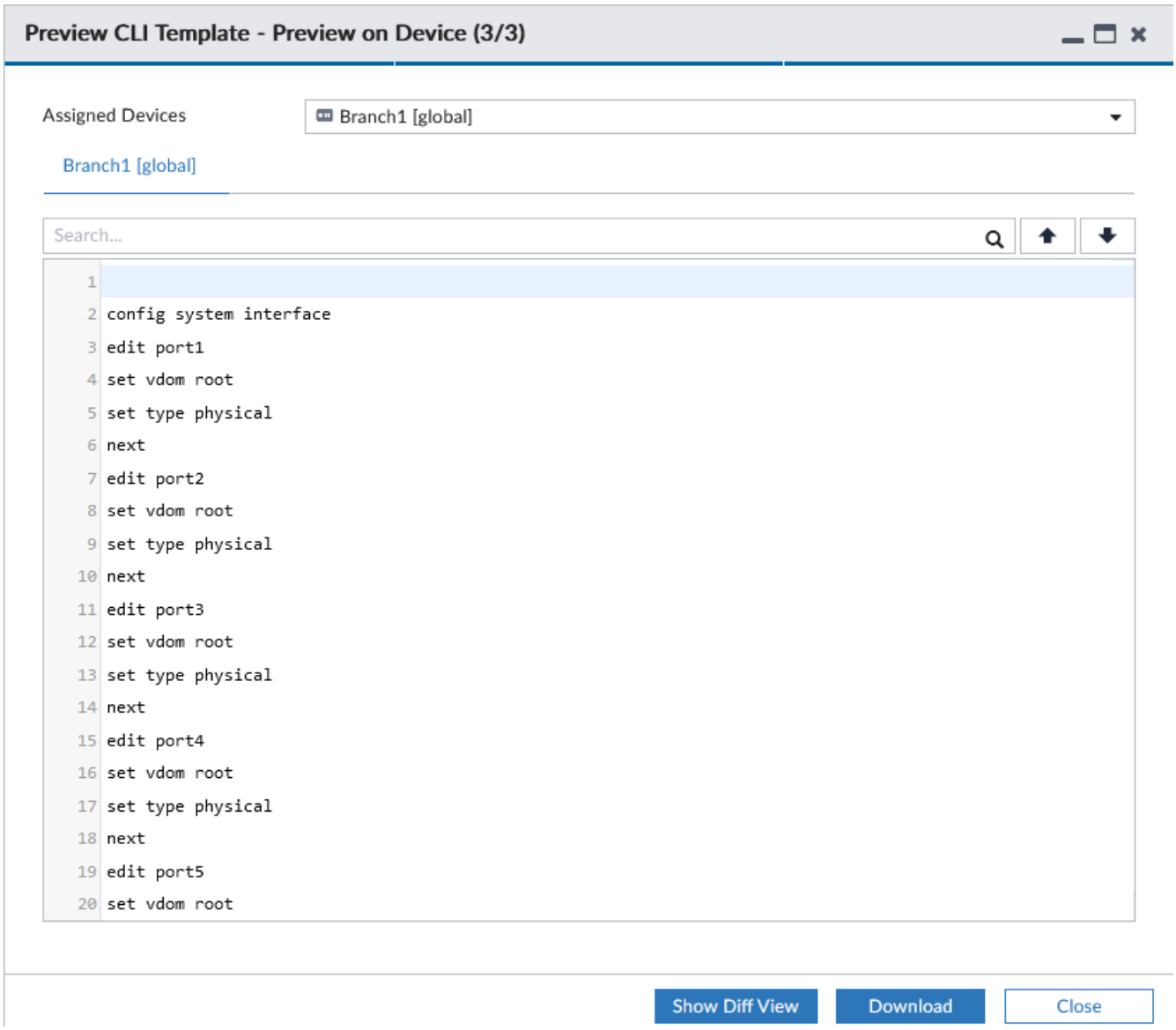
Using Jinja, the same CLI template can be applied to ANY new devices (hardware or VM-based) by using a script with FortiManager variables to determine the platform of the device and using an "if" statement to ensure that the script runs only on FortiGate-VM devices.

Example script:

```
{% if 'FortiGate-VM64' in DVMDB.platform -%}
config system interface
{%- for i in range(0, vm_interface_number|int) %}
edit port{{i+1}}
set vdom root
set type physical
next
{%- endfor %}
end
{%- endif %}
```



Previewing the script on a device shows how the variables are applied.



Example 2: View the device attributes for FortiGate-VMs

Example script:

```
{%- if DVMDB.platform == 'FortiGate-VM64' %}
Name: {{DVMDB.name}}
Serial: {{DVMDB.serial}}
OS TYPE: {{DVMDB.os_type}}
Platform: {{DVMDB.platform}}
Version: {{DVMDB.version}}
hostname: {{DVMDB.hostname}}
UUID: {{DVMDB.mgmt_uuid}}
Mgmt Interface IP : {{DVMDB.mgmt_if}}
IP: {{DVMDB.ip}}
Tunnel IP : {{DVMDB.tunnel_ip}}
Description: {{DVMDB.description}}
```

```
os_type: {{DVMDB.os_type}}
{%- endif %}
```

The rendered result for the script:

```
=======================
Name: vlan171_0040
Serial: FGVM08HZ20311040
OS TYPE: FortiGate
Platform: FortiGate-VM64
Version: 7.4.0
hostname: 3456-abc
UUID: 9c50812a-caa8-51ed-958a-4e7800e5139a
Mgmt Interface IP : port1
IP: 10.8.71.40
Tunnel IP : 169.254.0.12
Description:
os_type: FortiGate
```

Example 3: View the interface attributes for each physical interface on a device

Example script:

```
{%- for intf in DEVDB_system_interface %}
{%- if intf.type == 'physical' %}
Interface Name: {{intf.name}}
-- Interface Allowaccess: {{intf.allowaccess}}
-- Interface Type: {{intf.type}}
-- Interface IP: {{intf.ip}}
-- Interface Mode: {{intf.mode}}
-- Interface VDOM: {{intf.vdom}}
{%- endif %}
{%- endfor %}
```

The rendered result for the script:

```
==============================
Interface Name: port1
-- Interface Allowaccess: ping
-- Interface Type: physical
-- Interface IP: 10.8.71.40
-- Interface Mode: static
-- Interface VDOM: "root"
Interface Name: port2
-- Interface Allowaccess: https
-- Interface Type: physical
-- Interface IP: 101.71.40.1
-- Interface Mode: static
-- Interface VDOM: "root"
Interface Name: port3
-- Interface Allowaccess: ping
-- Interface Type: physical
-- Interface IP: 200.71.40.1
-- Interface Mode: static
-- Interface VDOM: "root"
Interface Name: port4
-- Interface Allowaccess:
-- Interface Type: physical
```

```
-- Interface IP: 0.0.0.0
-- Interface Mode: static
-- Interface VDOM: "root"
Interface Name: port5
-- Interface Allowaccess: ping
-- Interface Type: physical
-- Interface IP: 172.71.40.1
-- Interface Mode: static
-- Interface VDOM: "root"
Interface Name: port6
-- Interface Allowaccess:
-- Interface Type: physical
-- Interface IP: 0.0.0.0
-- Interface Mode: static
-- Interface VDOM: "root"
Interface Name: port7
-- Interface Allowaccess:
-- Interface Type: physical
-- Interface IP: 0.0.0.0
-- Interface Mode: static
-- Interface VDOM: "root"
Interface Name: port8
-- Interface Allowaccess:
-- Interface Type: physical
-- Interface IP: 0.0.0.0
-- Interface Mode: static
-- Interface VDOM: "root"
Interface Name: port9
-- Interface Allowaccess:
-- Interface Type: physical
-- Interface IP: 0.0.0.0
-- Interface Mode: static
-- Interface VDOM: "root"
Interface Name: port10
-- Interface Allowaccess:
-- Interface Type: physical
-- Interface IP: 0.0.0.0
-- Interface Mode: static
-- Interface VDOM: "root"
```

Fabric Authorization Template is integrated with Device Blueprint and supports meta variables - 7.4.1

This information is also available in the FortiManager 7.4 Administration Guide:

- Using Device Blueprints for Model Devices
- Fabric Authorization Templates

In FortiManager 7.4.1, the Fabric Authorization Template is integrated with Device Blueprints and supports metadata variables.

To use Fabric Authorization Templates with Device Blueprints:

Step 1: Configure the Fabric Authorization Template

To create a Fabric Authorization Template:

1. Go to *Device Manager* > *Provisioning Templates* > *Fabric Authorization.*
2. Click *Create New*, and the *Create New Fabric Authorization Template* dialog appears.
3. Configure the Fabric Authorization Template, for example a template named "60E" is configured in the with the following settings:
   a. FortiAP:

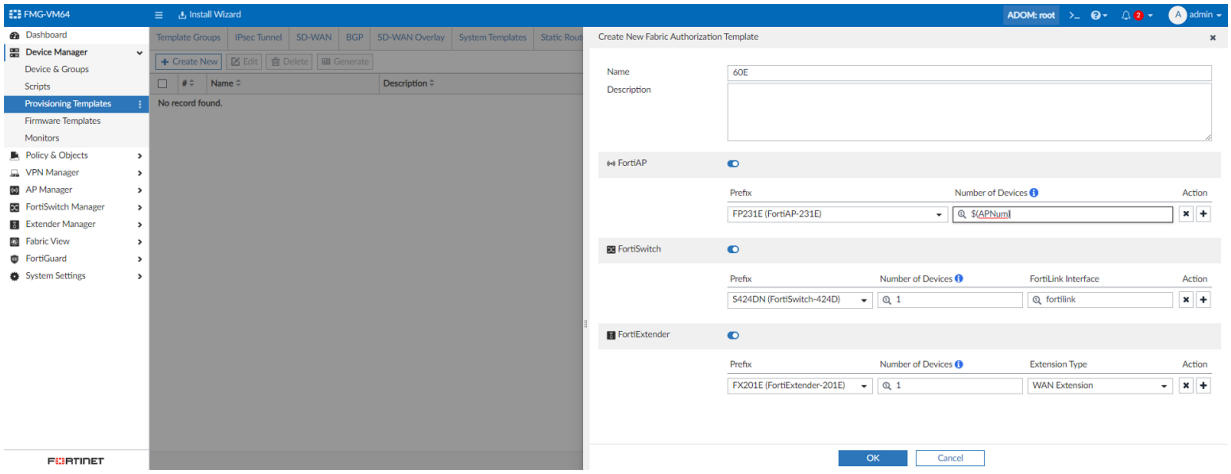
FortiAP	Toggle ON to enable FortiAP in the template.
Prefix	Select a model from the dropdown list, for example *FP231E*.
Number of Devices	This field determines how many APs will be added, and you can enter a number or use a variable. Entering the `$` sign causes the variable list to appear where you can select a variable from the dropdown list. This example uses the `$(APNum)` variable.

   b. FortiSwitch:

FortiSwitch	Toggle ON to enable FortiSwitch in the template.
Prefix	Select a model from the dropdown list, for example *S424DN*.
Number of Devices	This field determines how many FortiSwitches will be added, and you can enter a number or use a variable. This example uses the number `1`.
FortiLink Interface	Enter the interface name. This field supports variables. This example uses the name `fortilink`.

c. FortiExtender:

FortiExtender	Toggle ON to enable FortiExtender in the template.
Prefix	Select a model from the dropdown list, for example *FX201E*.
Number of Devices	This field determines how many FortiExtenders will be added, and you can enter a number or use a variable. This example uses the number `1`.
FortiLink Interface	Select an extension type from the dropdown list. This example uses *WAN Extension*.



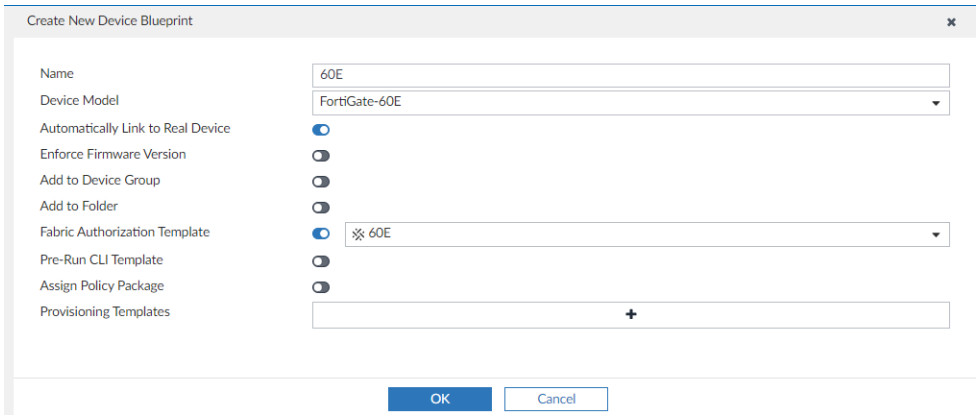
4. Click *OK* to save the Fabric Authorization Template.

Step 2: Add a Fabric Authorization Template to a device blueprint

To add the Fabric Authorization Template to a device blueprint:

1. Go to Device Manager. In the *Device & Group* window, click the *Add Device* dropdown and choose *Device Blueprint* to create a new device blueprint.
2. Configure the device blueprint. For example:

Name	Enter a name for the blueprint. In this example, it is `60E`.
Device Model	Select a device platform, for example *FortiGate-60E*.
Fabric Authorization Template	Select the previously configured Fabric Authorization Template (*60E*).



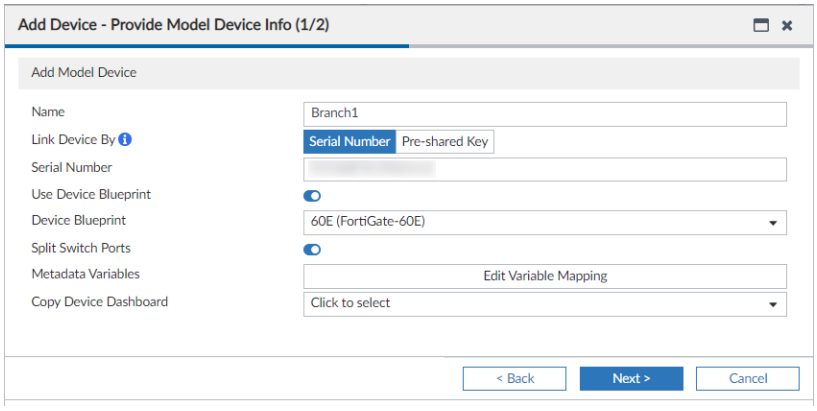
3. Click *OK* to save the device blueprint.

Step 3: Add the device blueprint to a model device

To add the Fabric Authorization Template to a model device:

1. Go to Device Manager. In the *Device & Group* window, click *Add Device* > *Add Model Device*.
2. Configure the model device using the device blueprint. For example:

Name	Enter the FortiGate's name. In this example, it is `Branch1`.
Link Device By	Select *Serial Number*.
Serial Number	Enter the serial number.
Use Device Blueprint	Enable the *Use Device Blueprint* setting.
Device Blueprint	Select the previously configured device blueprint (*`60E`*)

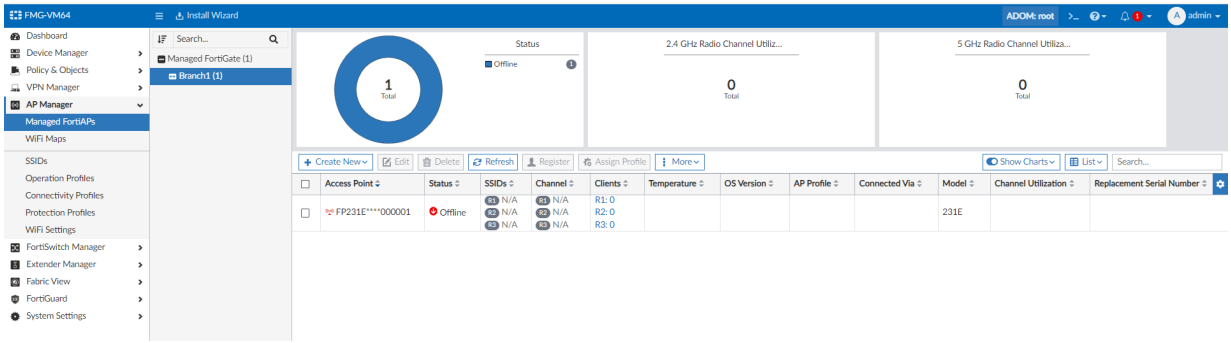


3. Click *OK* to save the model device.

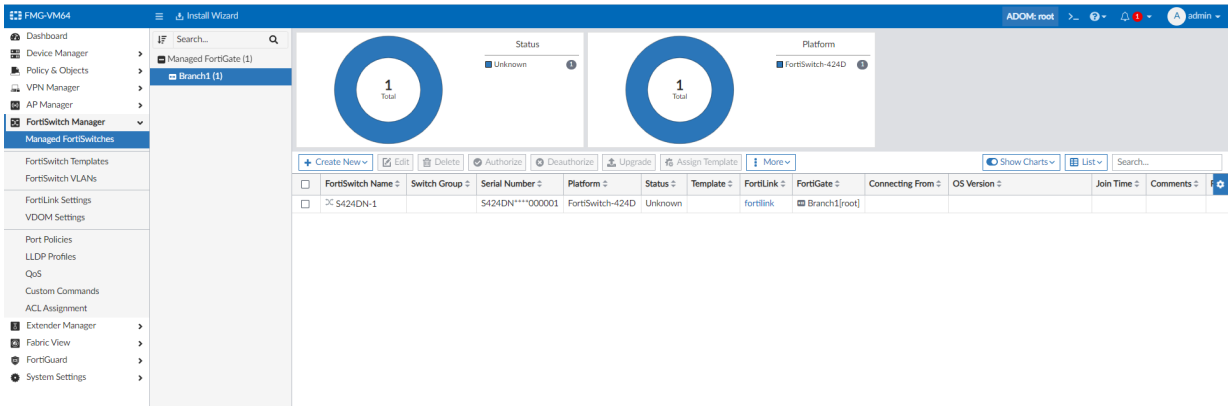
Step 4: View the configured FortiAP, FortiSwitch, and FortiExtender

1. After the device is added to the Device Manager, go to the *AP Manager*, *FortiSwitch Manager*, and *Extender Manager* in FortiManager and you can see that the FortiGate has been automatically configured with a FortiAP, FortiSwitch and FortiExtender as defined by the template.
   For example:

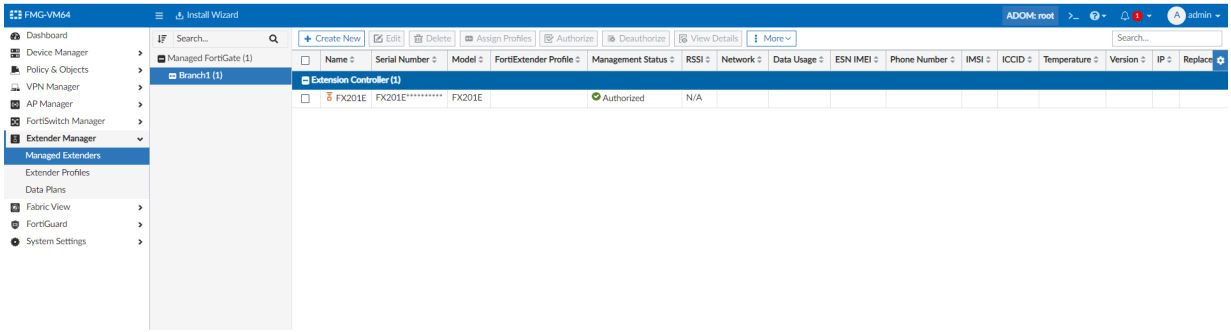
- FortiAP:



- FortiSwitch:



- FortiExtender:



Central Management

This section lists the new features added to FortiManager for central management:

AP Manager

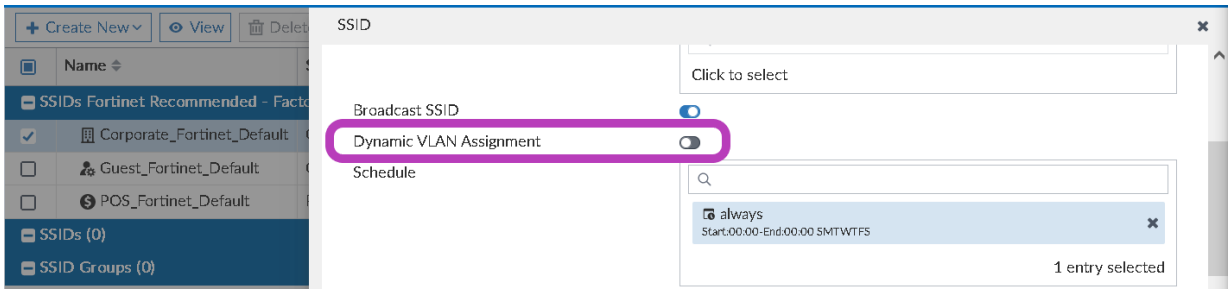
This section lists the new features added to FortiManager for AP manager:

Multiple optimizations to the factory default SSID and AP-profiles - 7.4.1

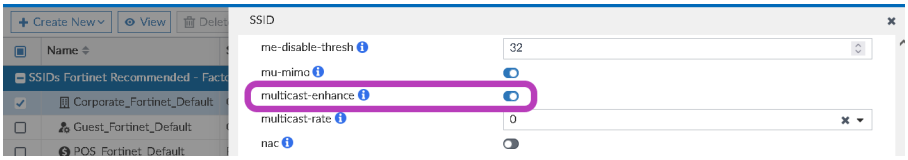
In FortiManager 7.4.1, there are multiple optimizations to the factory default SSID and AP-profiles.

Fortinet recommended factory default SSIDs

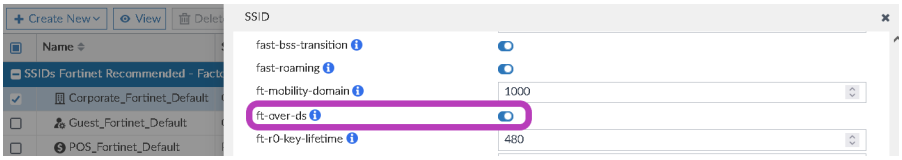
- All three Fortinet recommended factory default SSID templates allow users to select the traffic mode as either Bridged or Tunnel when the templates are activated.
- The *Corporate_Fortinet_Default* SSID includes the following changes:
  - *Dynamic VLAN Assignment* - disabled by default.



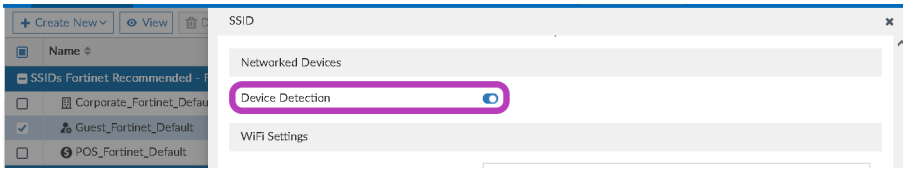
  - *multicast-enhance* - enabled by default.



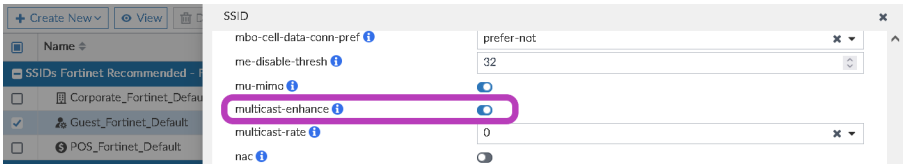
- *ft-over-ds* - enabled by default.



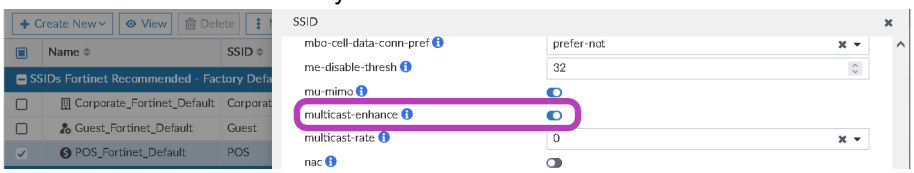
- The *Guest_Fortinet_Default* SSID includes the following changes:
  - *Device Detection* - enabled by default.



  - *multicast-enhance* - enabled by default.

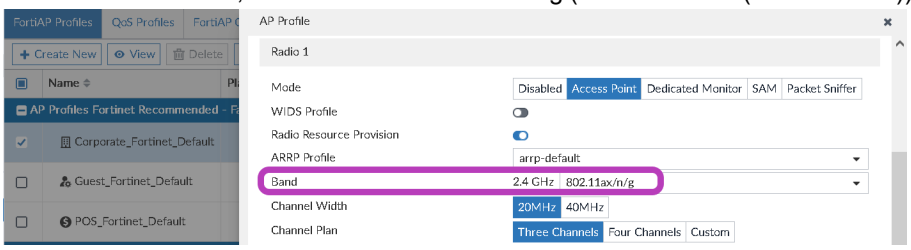


- The *POS_Fortinet_Default SSID* includes the following changes:
  - *multicast-enhance* - enabled by default.

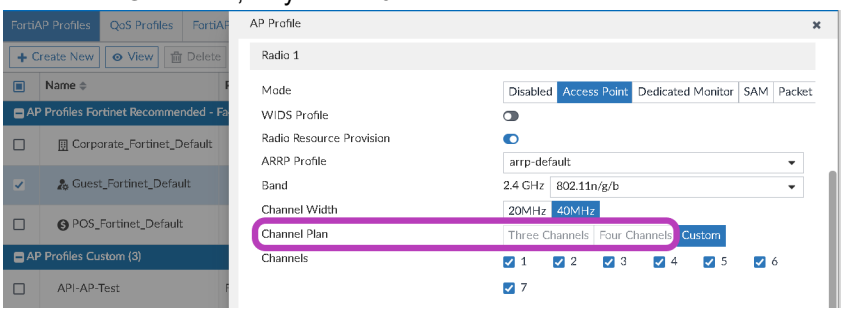


Fortinet recommended factory default AP Profiles

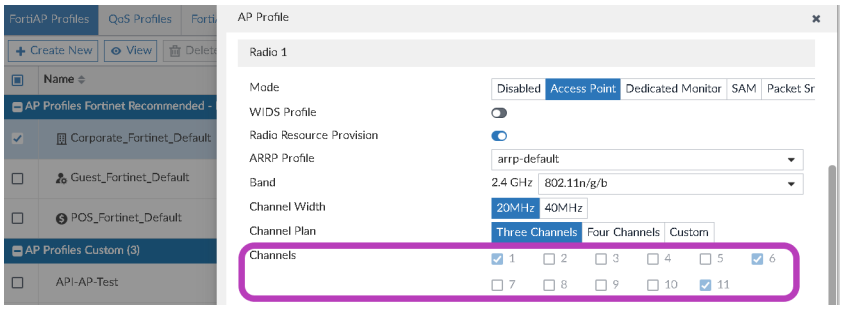
- For the 2.4 GHz band, set the default 802.11 ax/n/g (for WiFi6/6E/6 (Smart Series)).



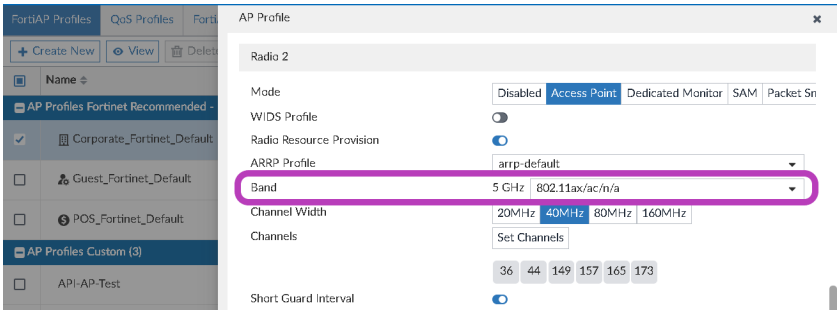
- For the 2.4 GHz band, only allow 20MHz channel width.



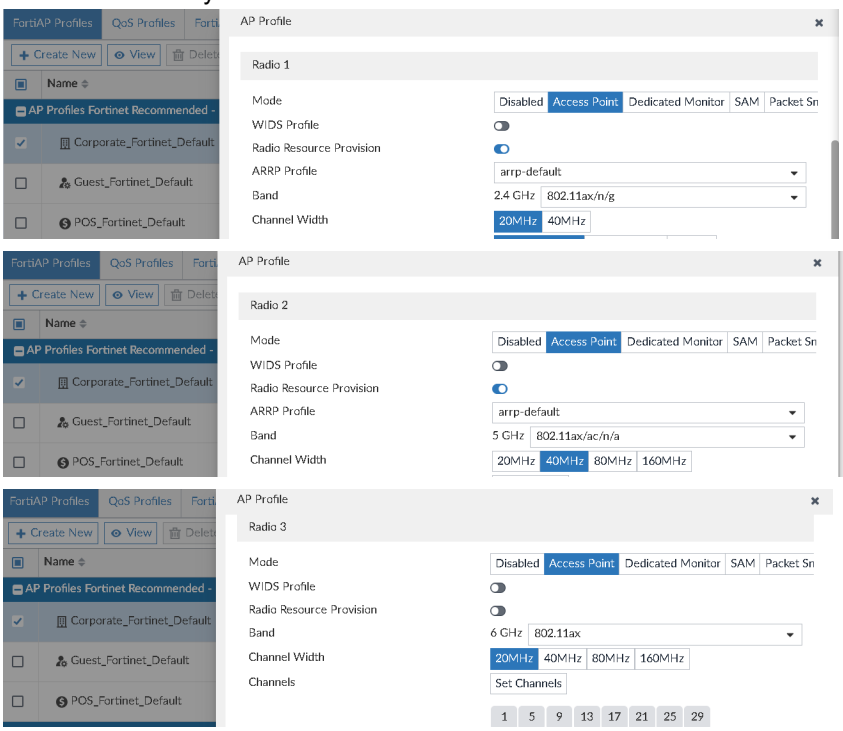
- Enforce the 2.4 GHz radio 1 on *Three Channels* (some profiles are on three channels "custom").



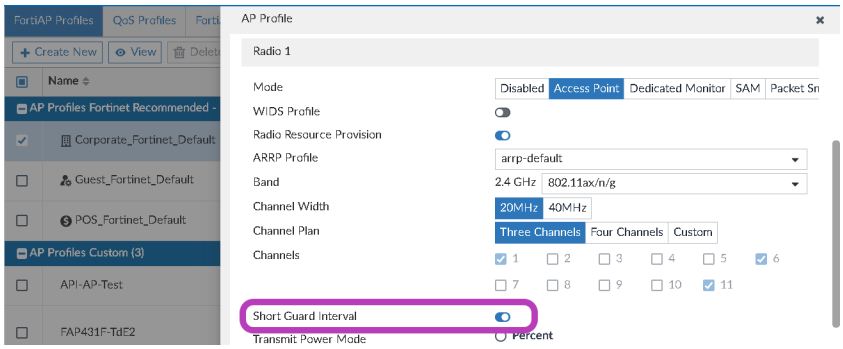
- For the 5 GHz band (radio 2), set to 802.11 ax/ac/n/a (for WiFi6/6E/6 (Smart Series)).



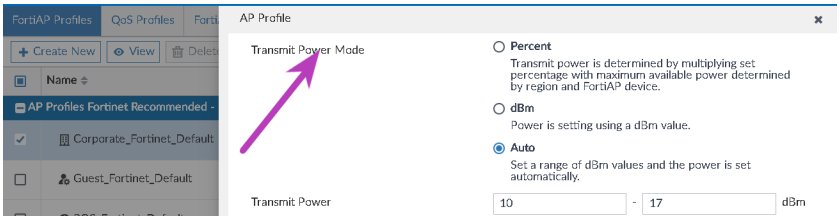
- Enable all radios by default.



- *Short Guard Interval* - enabled by default on all radios.

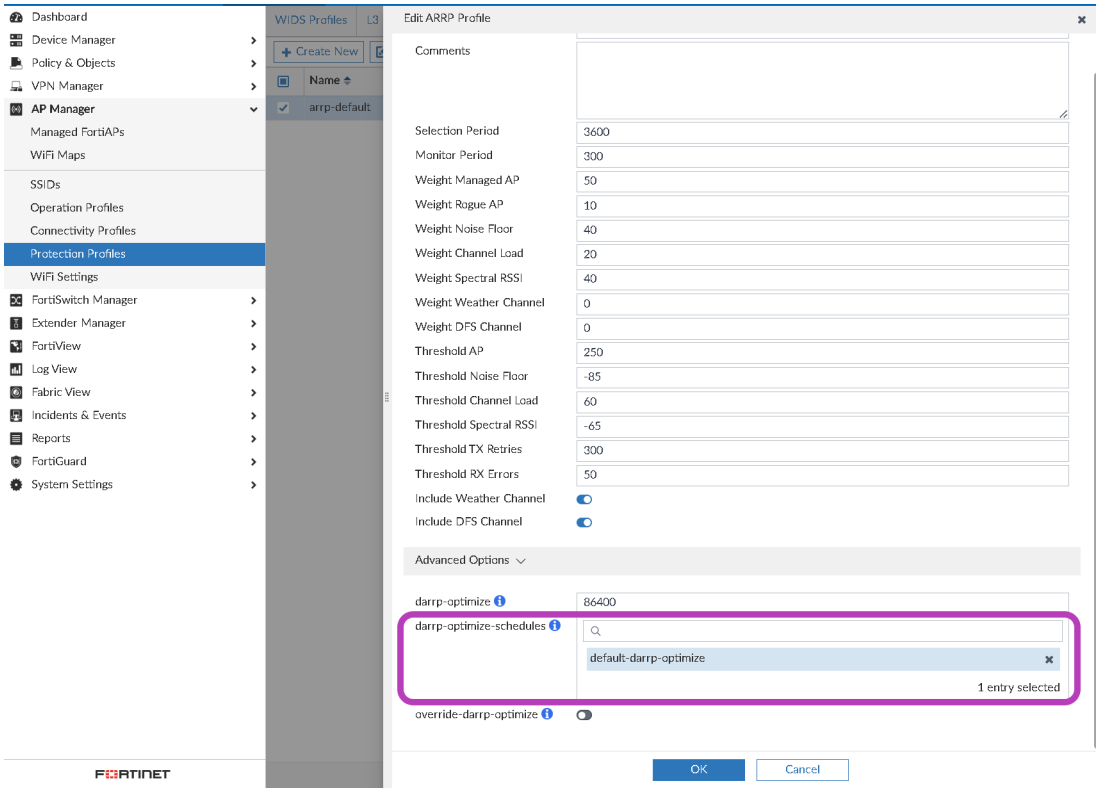


- *Transmit Power Mode* - set to *Auto* by default on all radios.



Fortinet recommended factory default ARRP Profile

- *darrp-optimize-schedules* - The *default-darrp-optimize* schedule in the profile is selected by default.



FortiSwitch Manager

This section lists the new features added to FortiManager for FortiSwitch manager:

Per-device VRRP mapping can be used under FortiSwitch Profiles

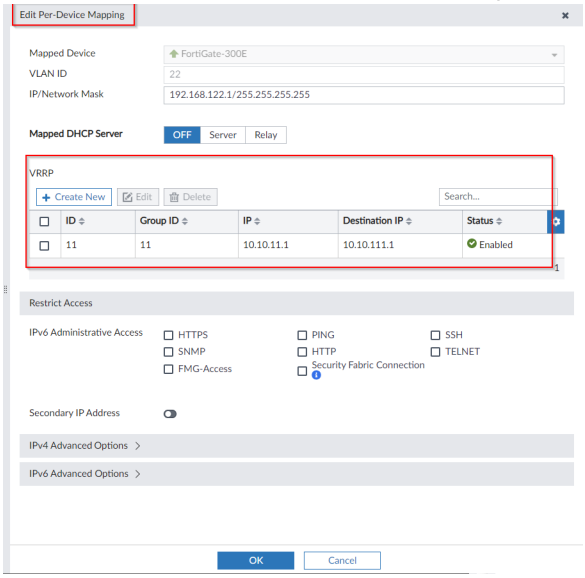
This information is also available in the FortiManager 7.4 Administration Guide:

- Creating FortiSwitch VLANs

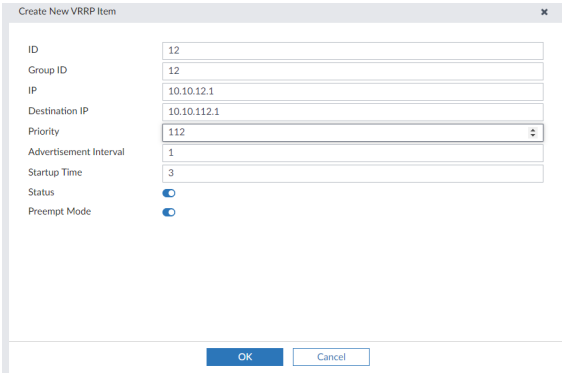
FortiManager supports per-device mapping for Virtual Router Redundancy Protocol (VRRP) in FortiSwitch profiles.

To configure per-device mappings for VRRP settings in a FortiSwitch profile:

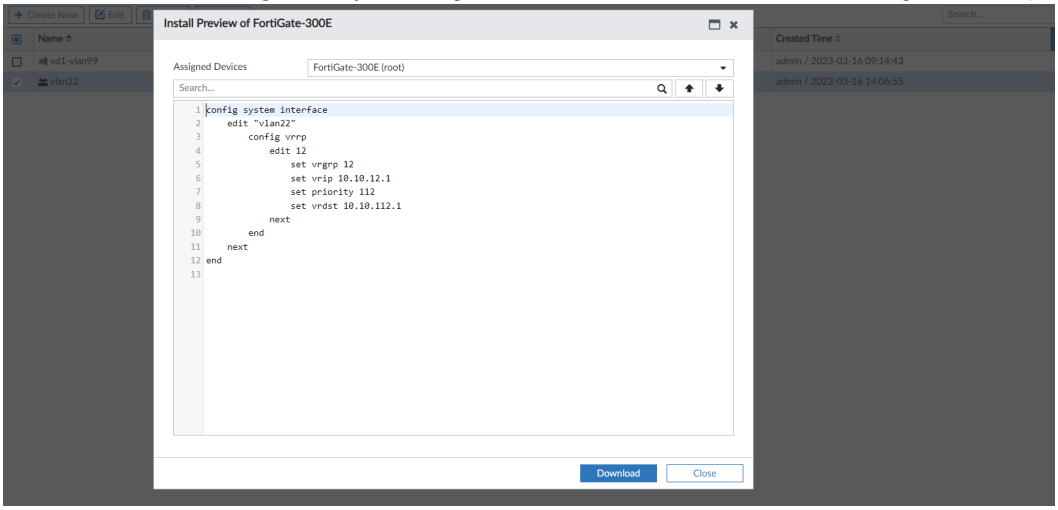
1. Go to *FortiSwitch Manager > FortiSwitch VLANs*.
2. Create or edit a VLAN interface, and make a per-device mapping for a FortiGate.



3. In the per-device mapping page, users can add a VRRP setting for the FortiSwitch VLAN.



4. When the VLAN is being used by an assigned FortiSwitch VLAN, the VRRP setting can be deployed.



FortiManager allows switchport export to another VDOM, and configuration of the exported port in the destination VDOM

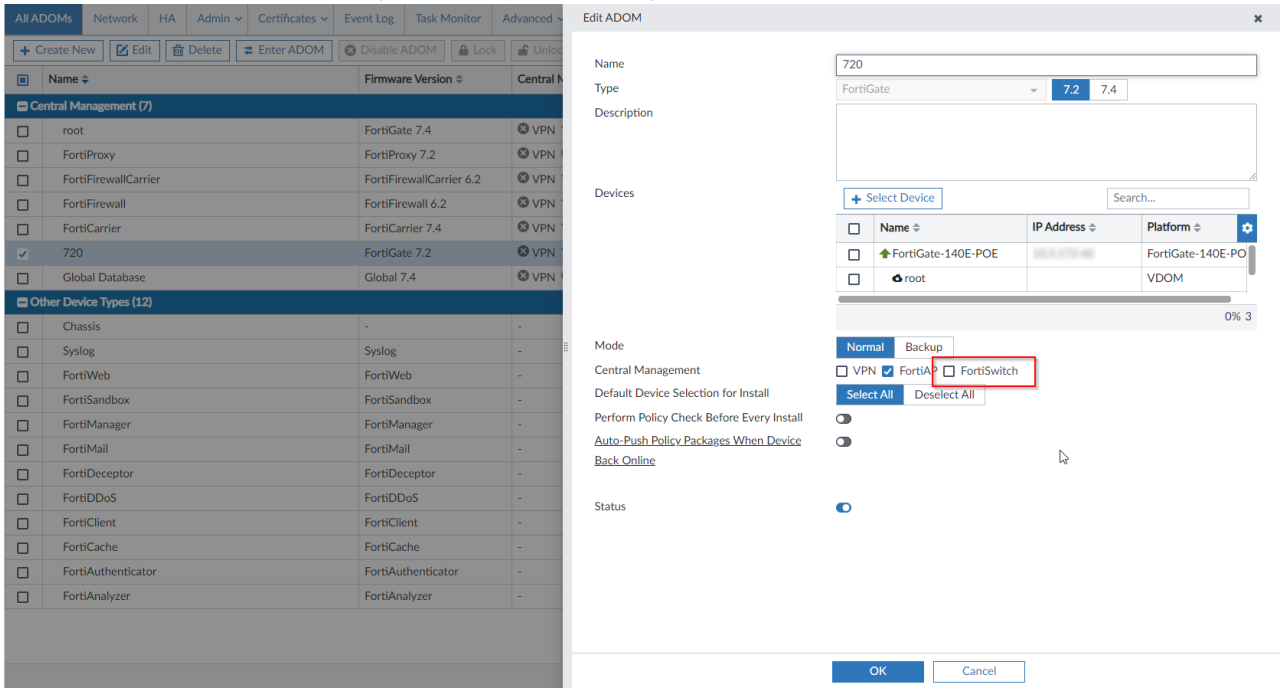
This information is also available in the FortiManager 7.4 Administration Guide:

- Exporting FortiSwitch ports to another VDOM

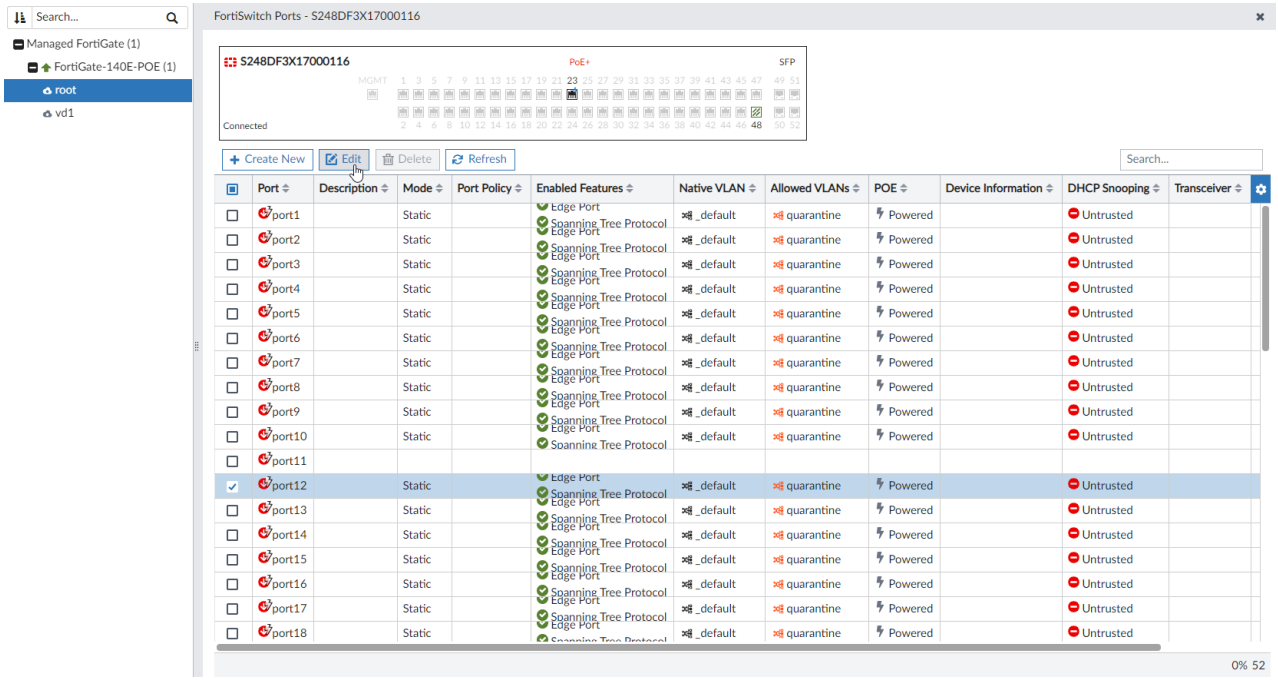
FortiManager allows switchport export to another VDOM, and configuration of the exported port in the destination VDOM.

To export FortiSwitch ports:

1. Disable *FortiSwitch Central Management* in *System Settings* > *All ADOMs*.

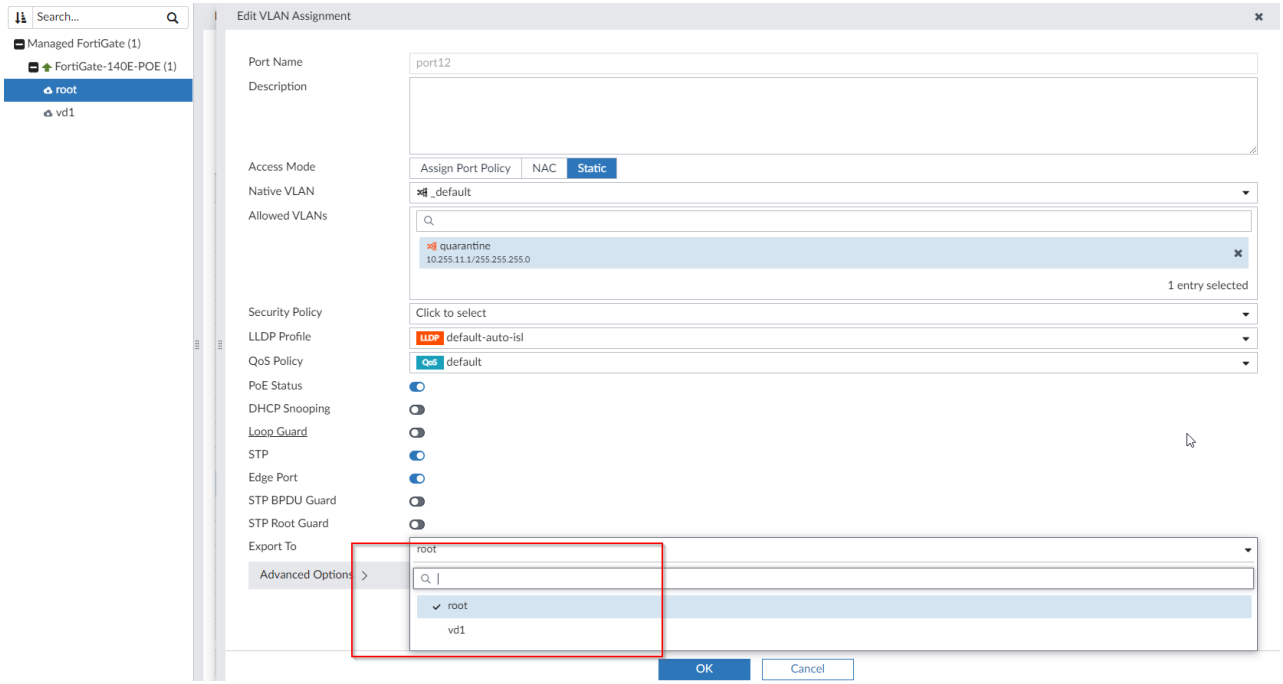


2. Add a Multi-VDOM enabled FortiGate with an attached FortiSwitch.

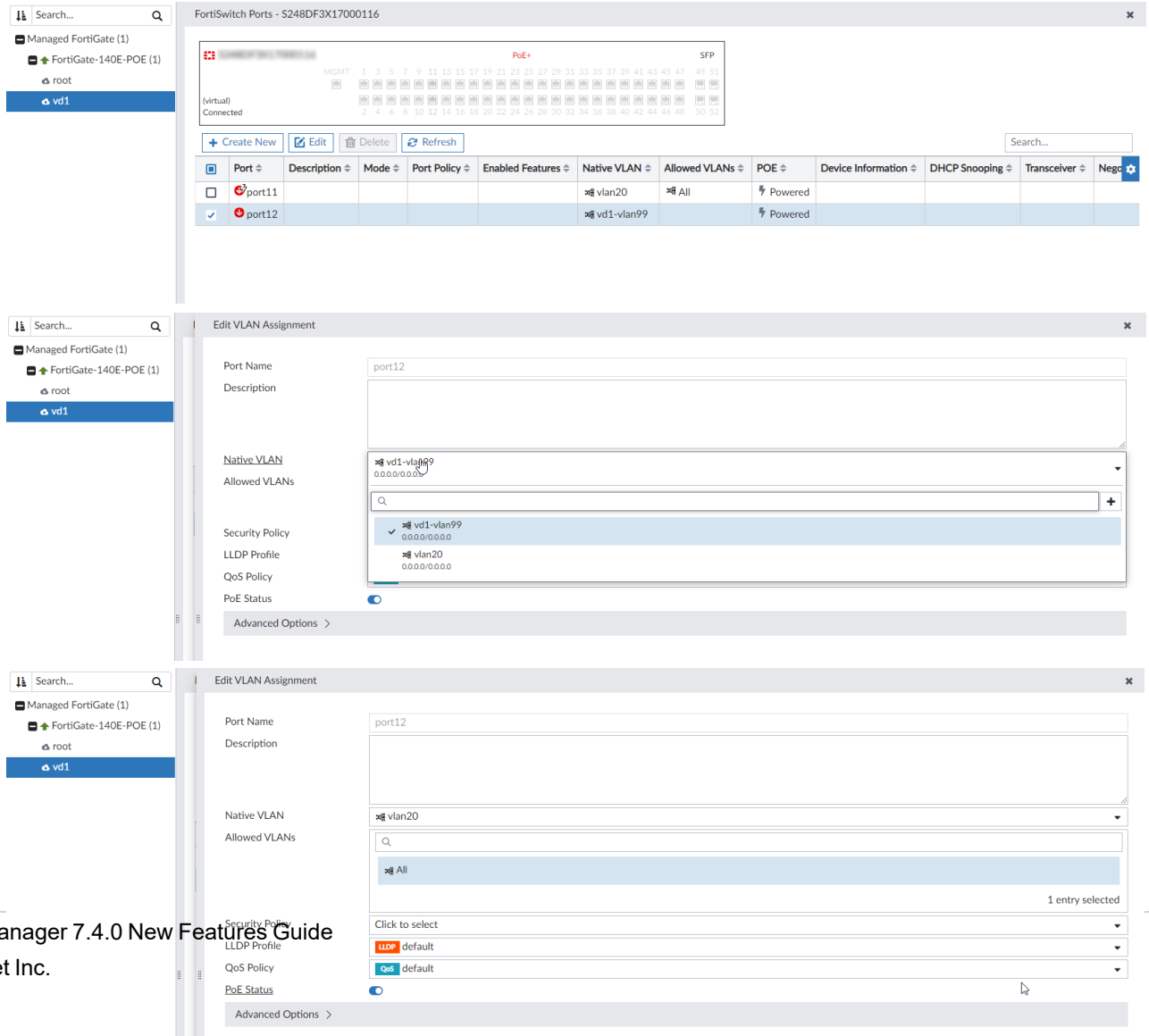


3. Go to *FortiSwitch Manager* > *Managed FortiSwitches*, right-click on a FortiSwitch and select *Ports Configuration*.

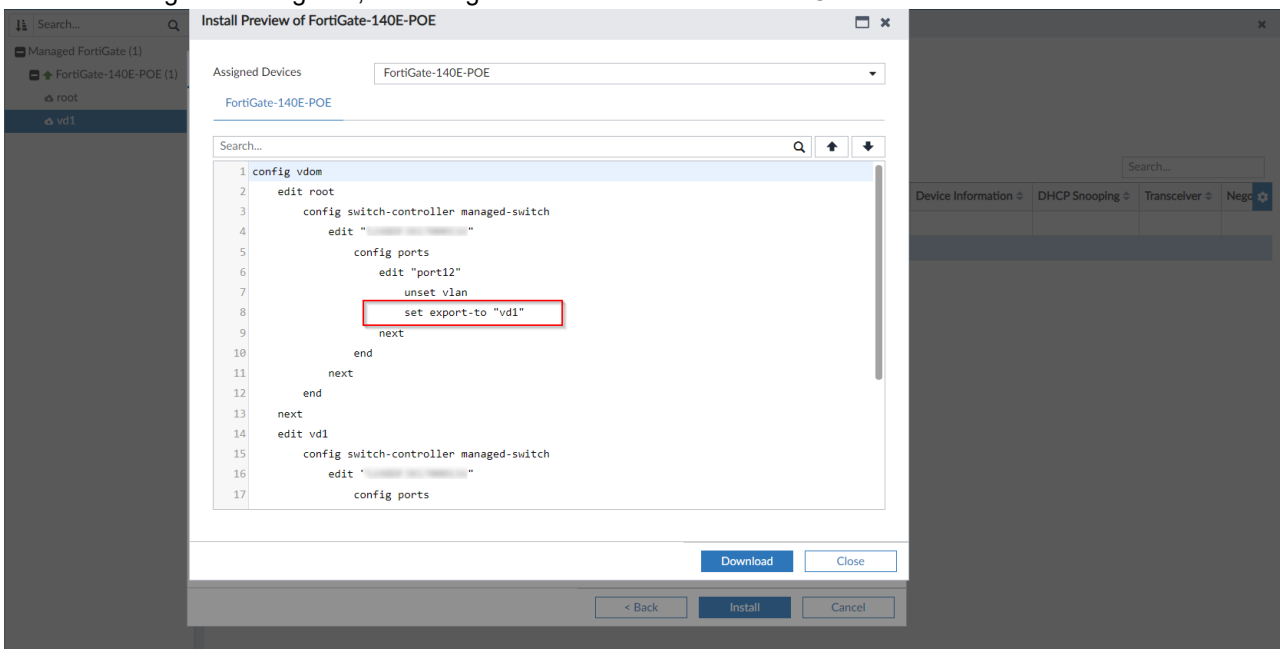
4. Edit a port to enter the *Edit VLAN Assignment* pane, and choose the new VDOM in the *Export To* field.



5. After the port is exported, users can edit the port's configuration in the chosen VDOM.



6. After the settings are configured, the changes can be installed to the FortiGate.



FortiSwitch replacement procedure can be executed from FortiManager GUI

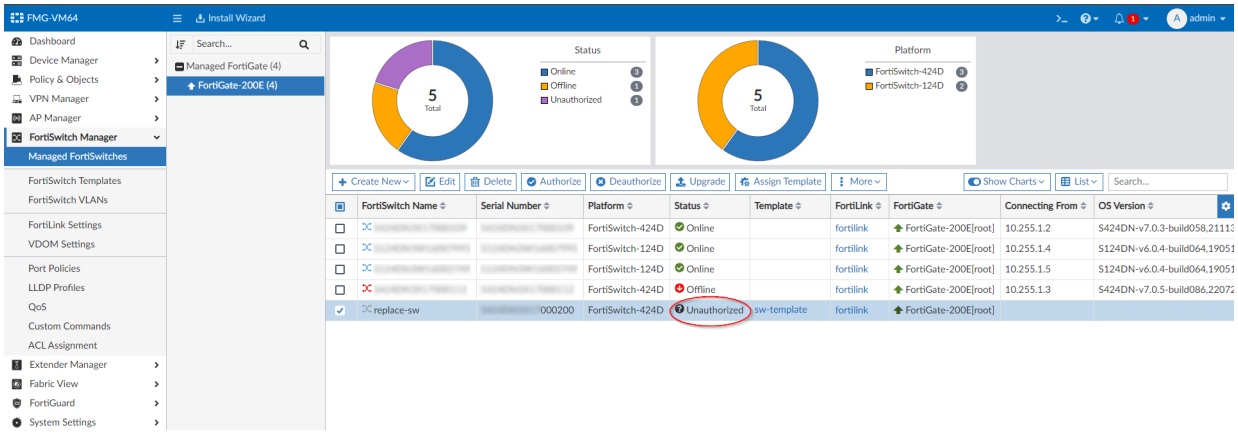
FortiSwitch replacement procedure can be executed from the FortiManager GUI.

This information is also available in the FortiManager 7.4 Administration Guide:

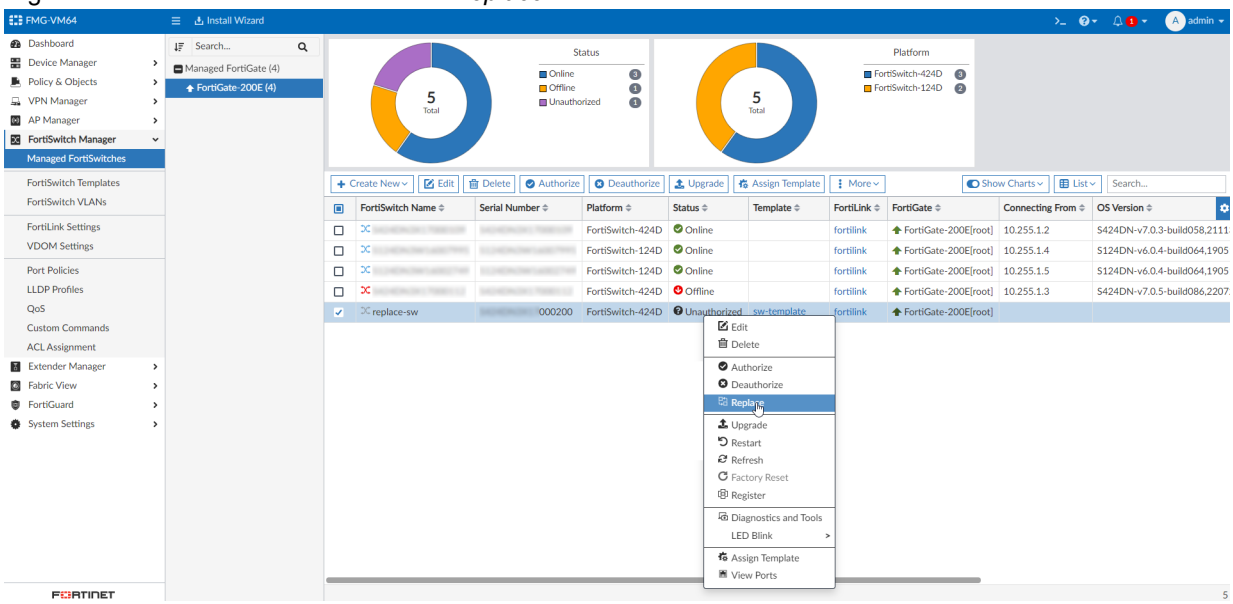
- Replacing Switches

To replace a FortiSwitch device from the FortiManager GUI:

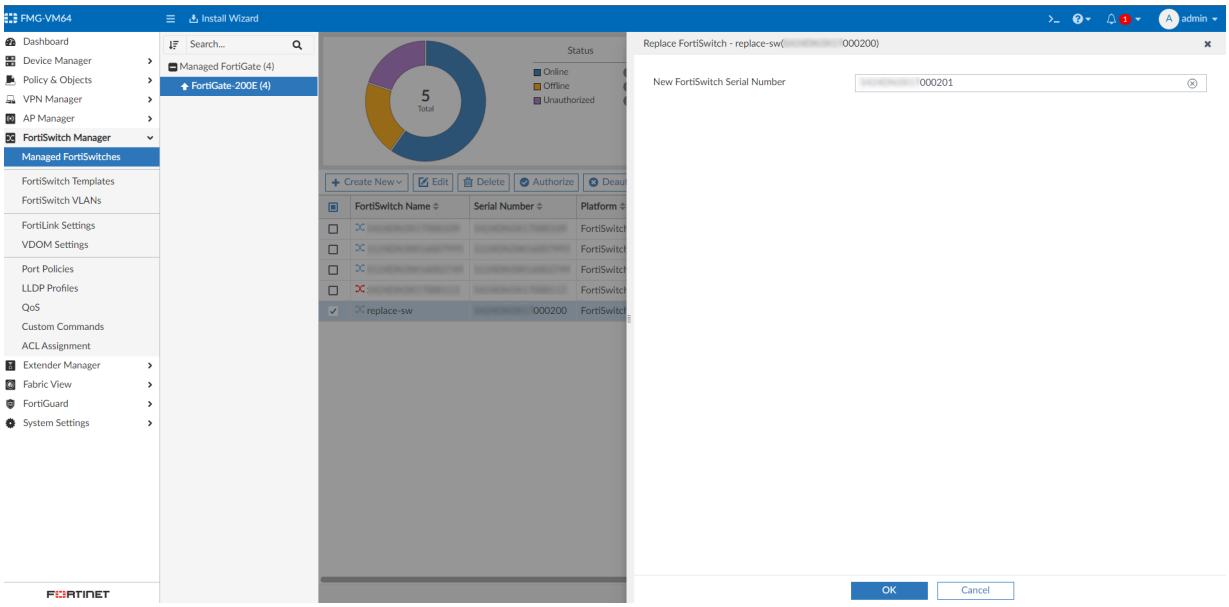
1. Go to *FortiSwitch Manager* > *Managed FortiSwitches*.
2. Deauthorize the FortiSwitch that will be replaced, and refresh the FortiSwitch list. The FortiSwitch will display with the status *Unauthorized*.



3. Right-click on the FortiSwitch and select *Replace*.

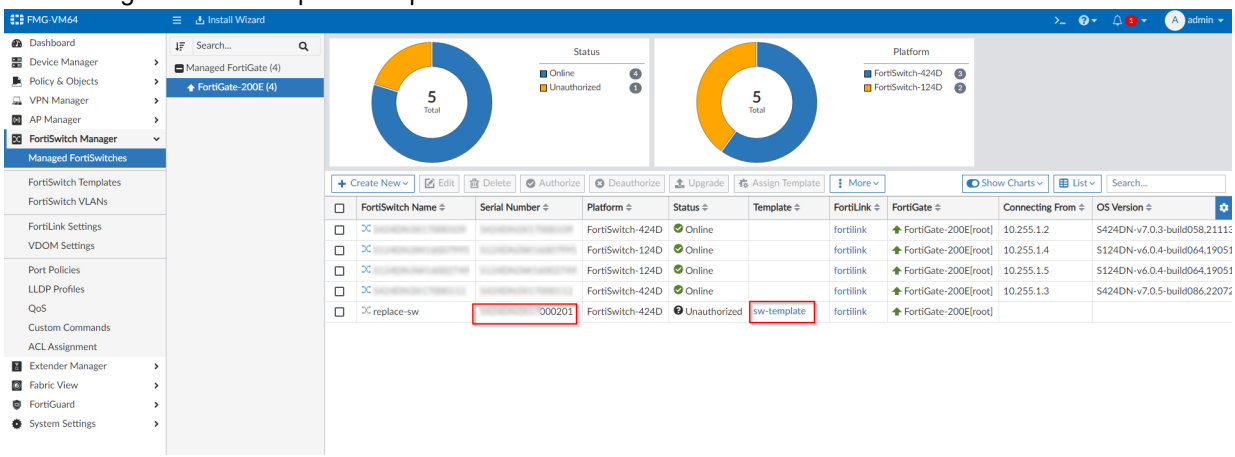


4. Enter the new FortiSwitch serial number, and click *OK* to confirm.

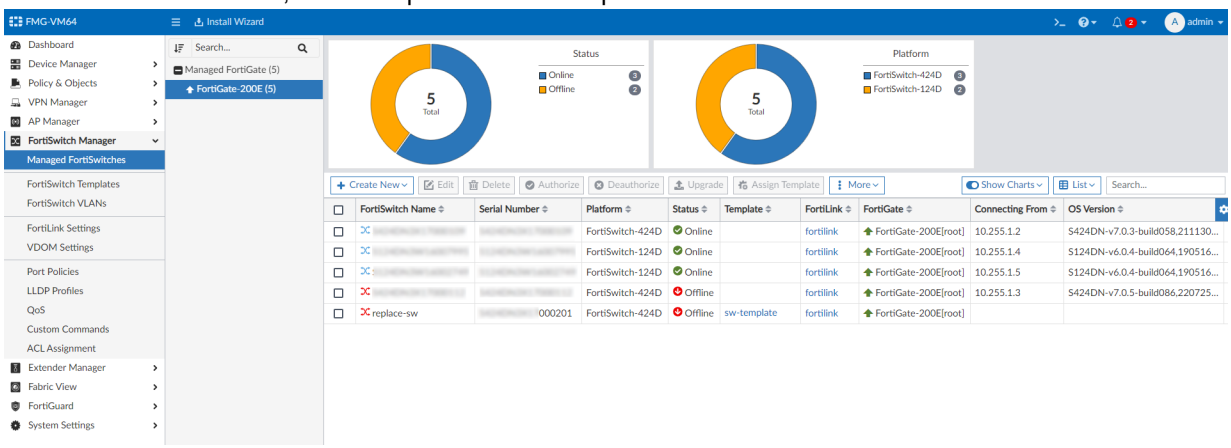


After the operation is complete, refresh the FortiSwitch list. The new FortiSwitch serial number will be displayed,

and the original switch template is kept.



5. Authorize the FortiSwitch, and the replacement is complete.



Custom commands can be assigned/unassigned at once to multiple managed FortiSwitches - 7.4.1

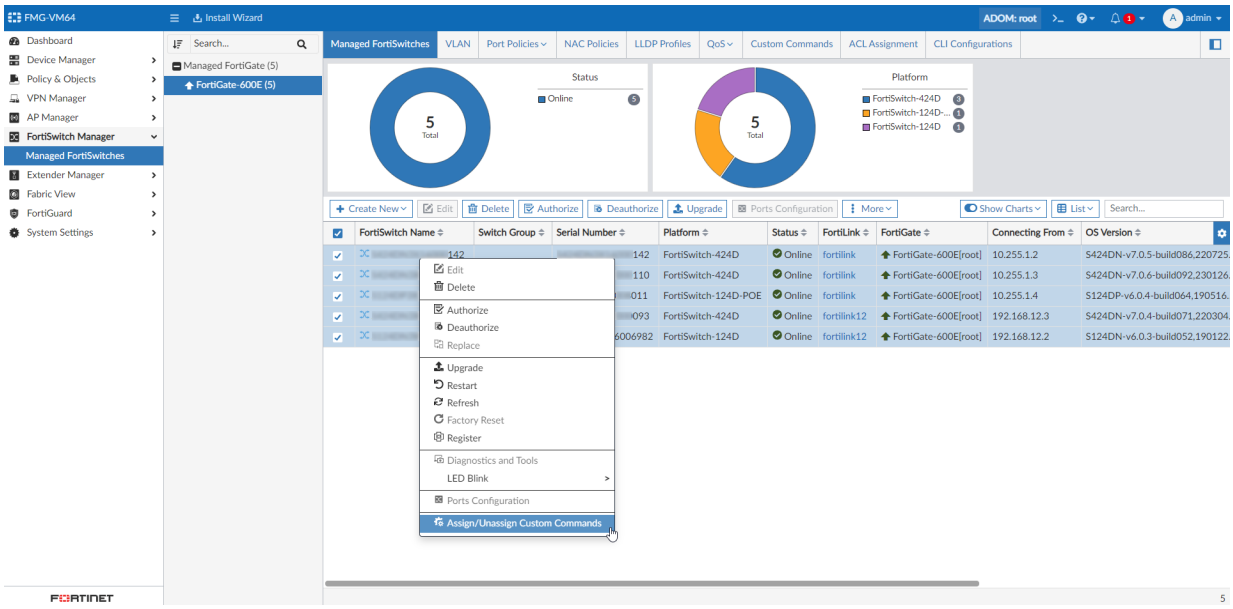
This information is also available in the FortiManager 7.4 Administration Guide:

- Creating custom commands

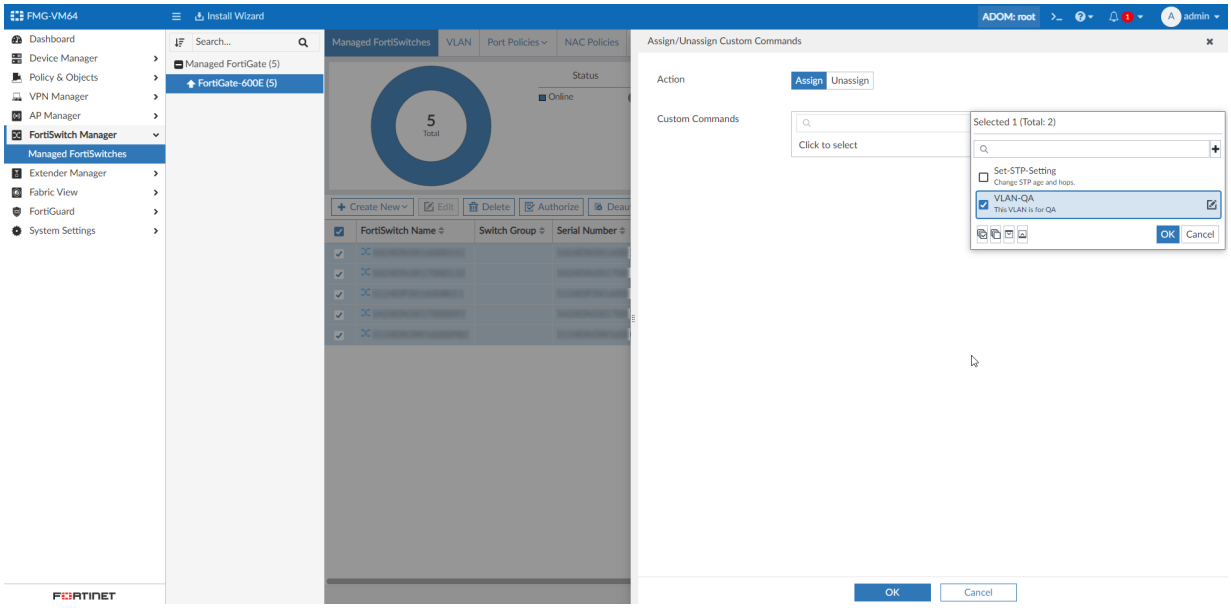
Custom commands can be assigned/unassigned at once to multiple managed FortiSwitches.

To push custom commands to multiple FortiSwitch devices:

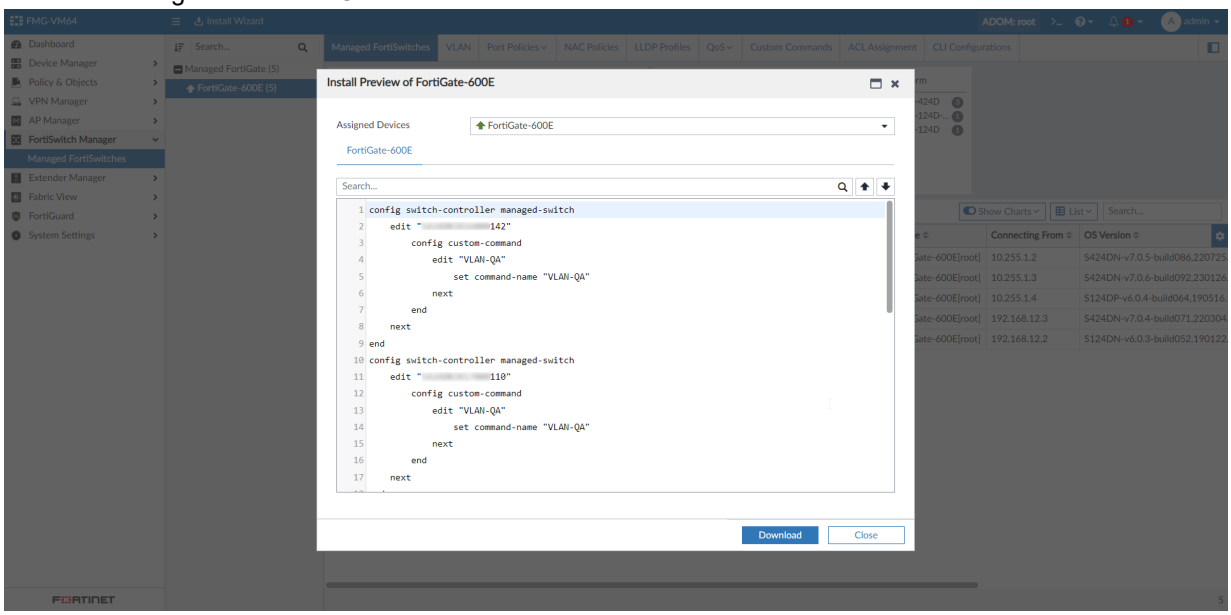
1. In Per-Device FortiSwitch management mode, select the FortiSwitch devices to which you want to assign custom commands. Multiple FortiSwitch devices can be selected at once.



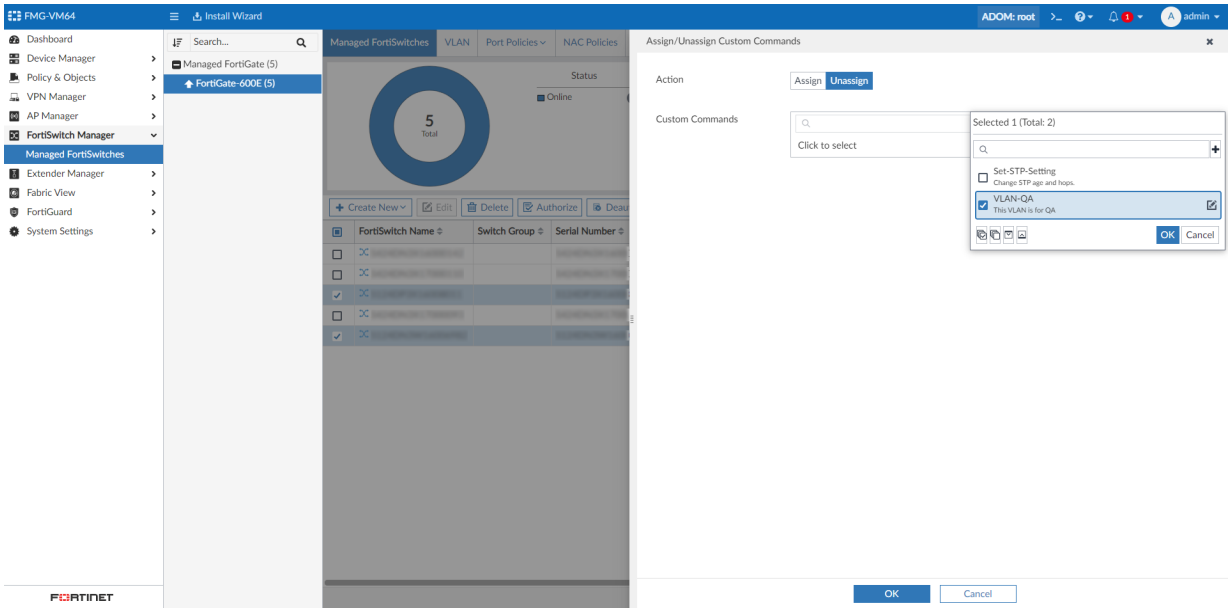
2. Right-click in the table and select *Assign/Unassign Custom Commands* from the context menu.
   The *Assign/Unassign Custom Commands* dialog appears.
3. Assign custom commands:
   a. Select the *Assign* tab and choose the custom command from the dropdown list.
   b. Click *OK*.



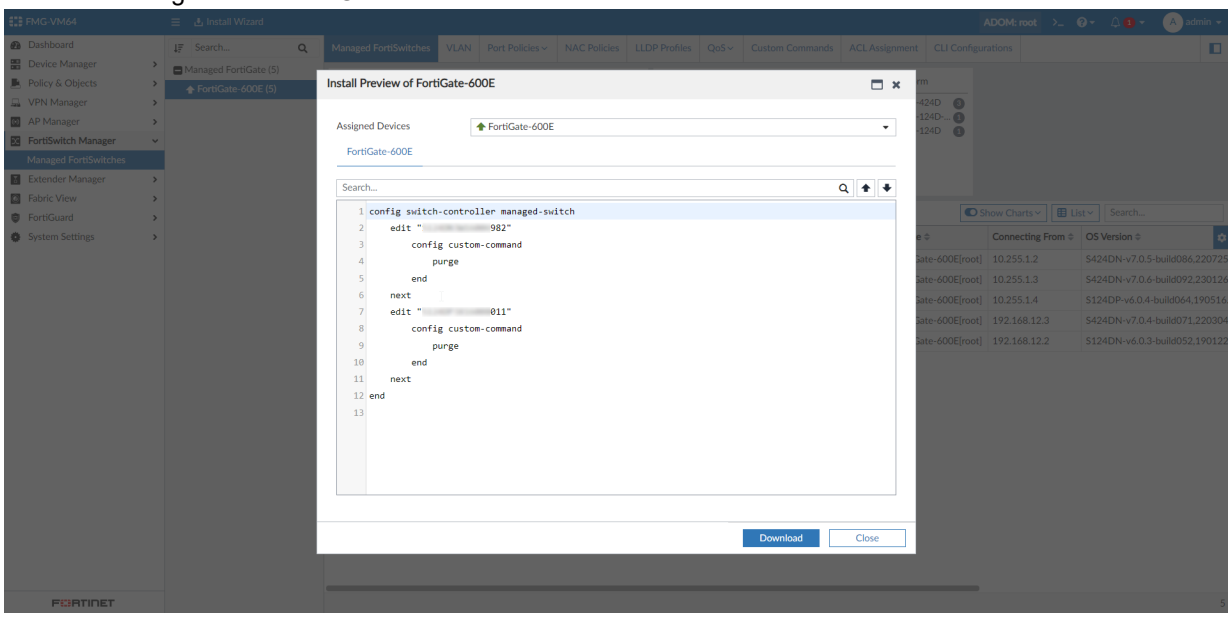
c. Install the changes to the FortiGate devices.



4. Unassign custom commands:
   a. Select the *Unassign* tab and choose the custom command from the dropdown list.
   b. Click *OK*.



c. Install the changes to the FortiGate devices.



Others

This section lists the new features added to FortiManager for other topics relating to central management:

- FortiManager supports install preview for model devices on page 59
- VPN Monitoring displays IPsec VPN tunnels created by IPsec templates and SD-WAN overlay wizard on page 64
- FortiManager supports CLI diff in the workflow approval sessions on page 67

FortiManager supports install preview for model devices

This information is also available in the FortiManager7.4 Administration Guide:

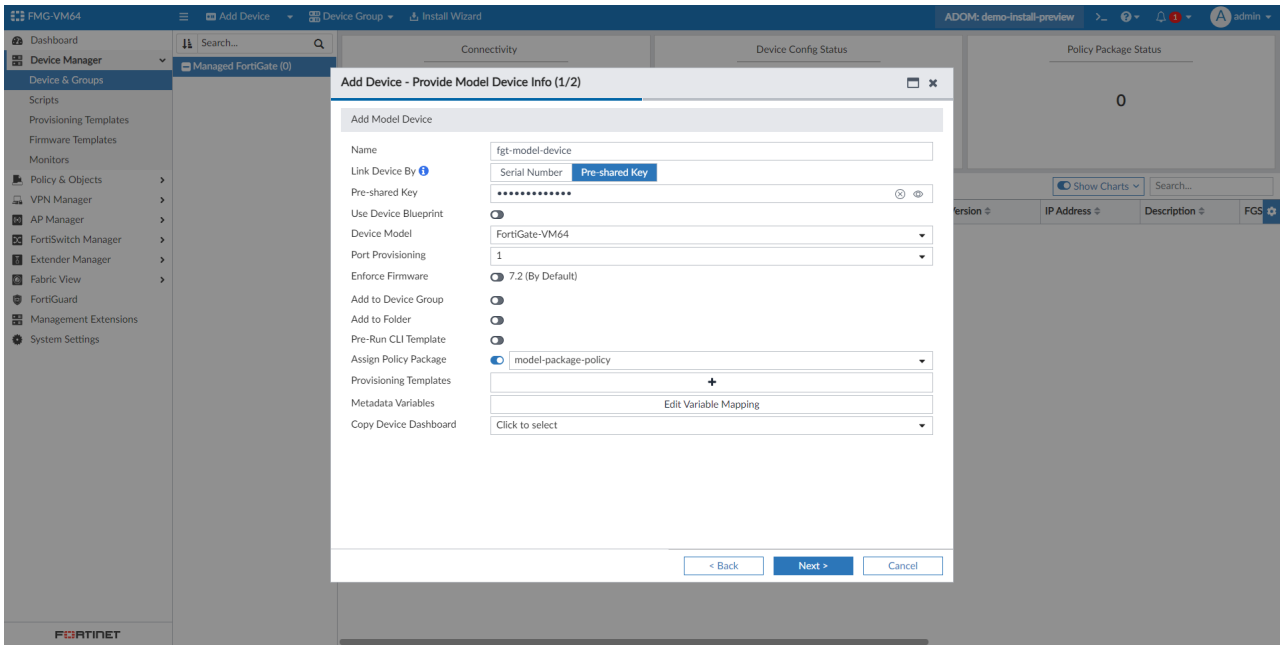
- Installing policy packages and device settings

Use the *Install Preview* feature in the *Install Wizard* to preview the configuration that will be applied to a model device.

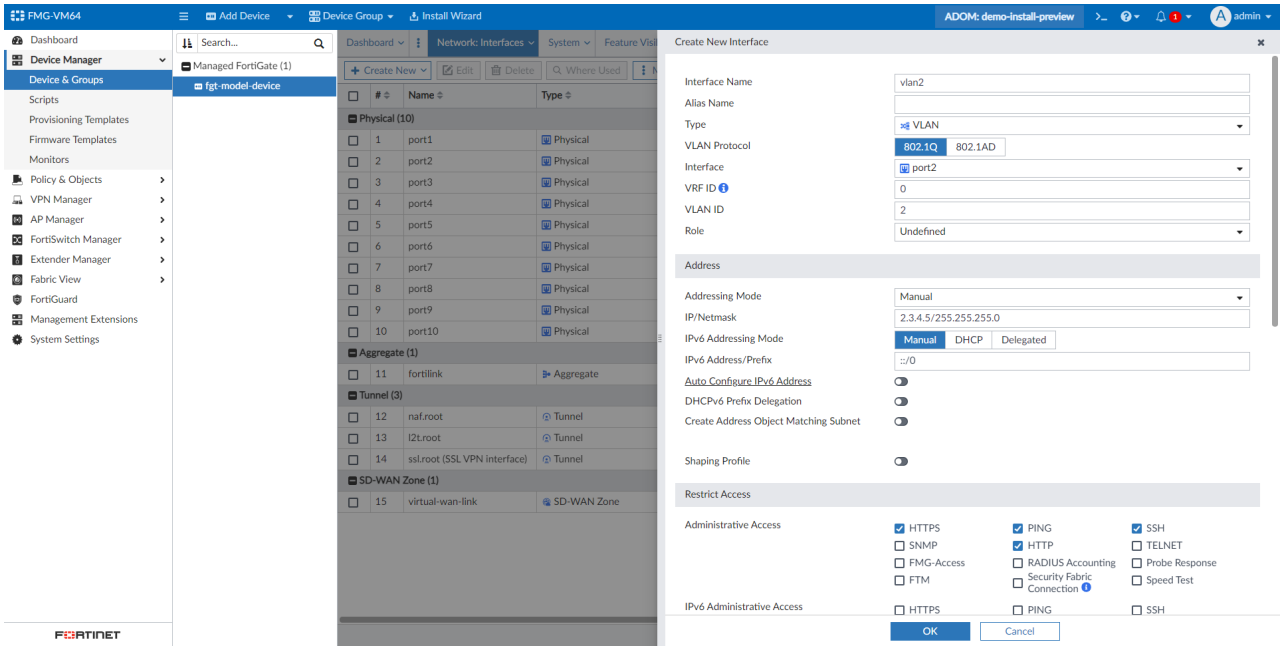
You can make changes to a model device in *Device Manager* or to a policy package that is applied to a model device in *Policy and Objects*. These changes will be saved to the local database of the model device in FortiManager. To preview the actual changes that will be applied, *Install Preview* can be accessed from the *Install Wizard*.

To use *Install Preview* for a model device:

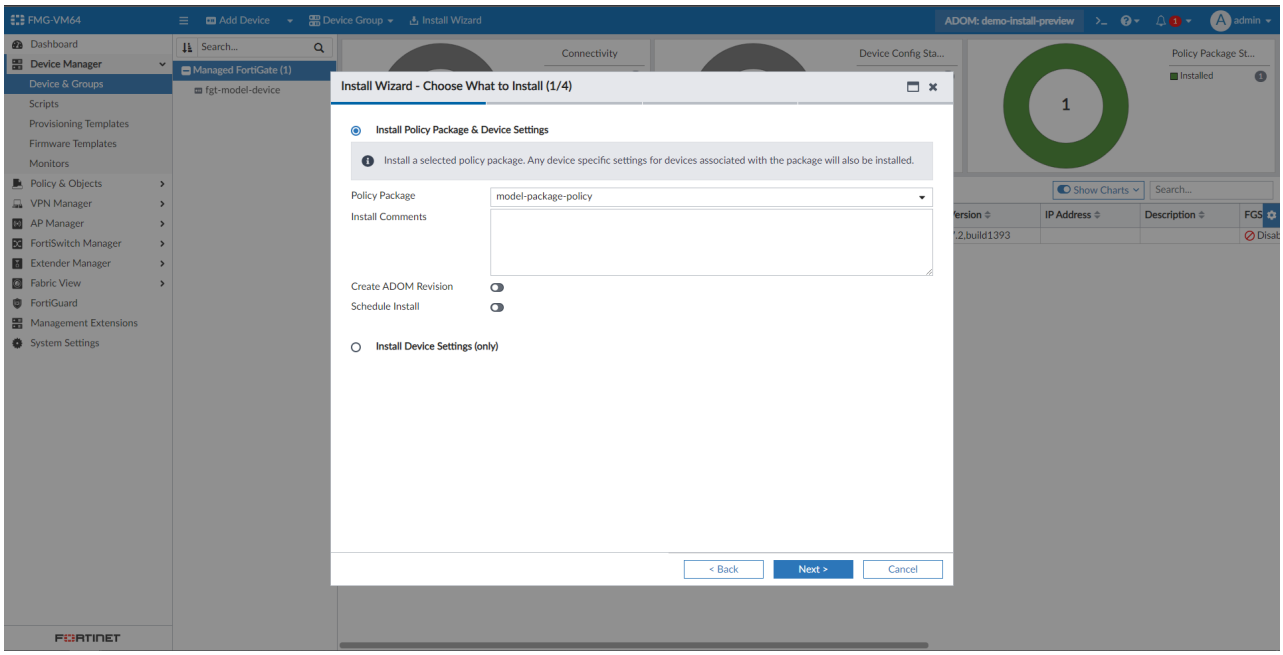
1. Add a model device through *Add Device* > *Add Model Device*. Assign a policy package.



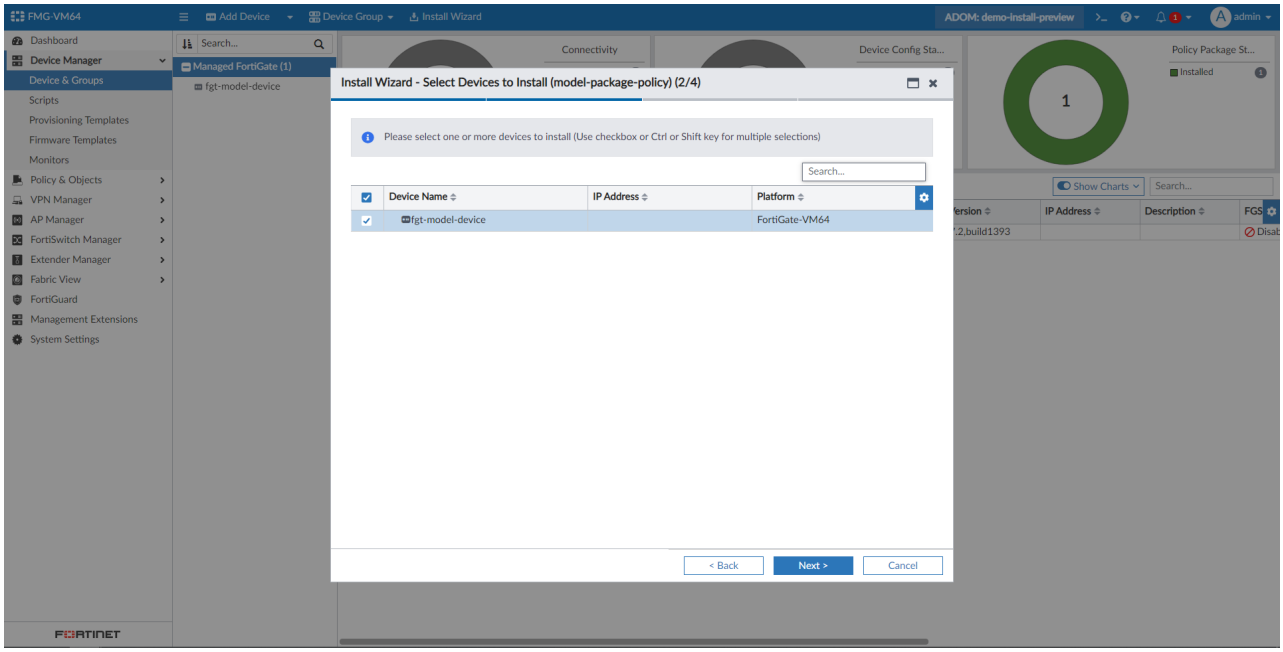
2. Make changes in *Device Manager*. In this example, create a VLAN interface.



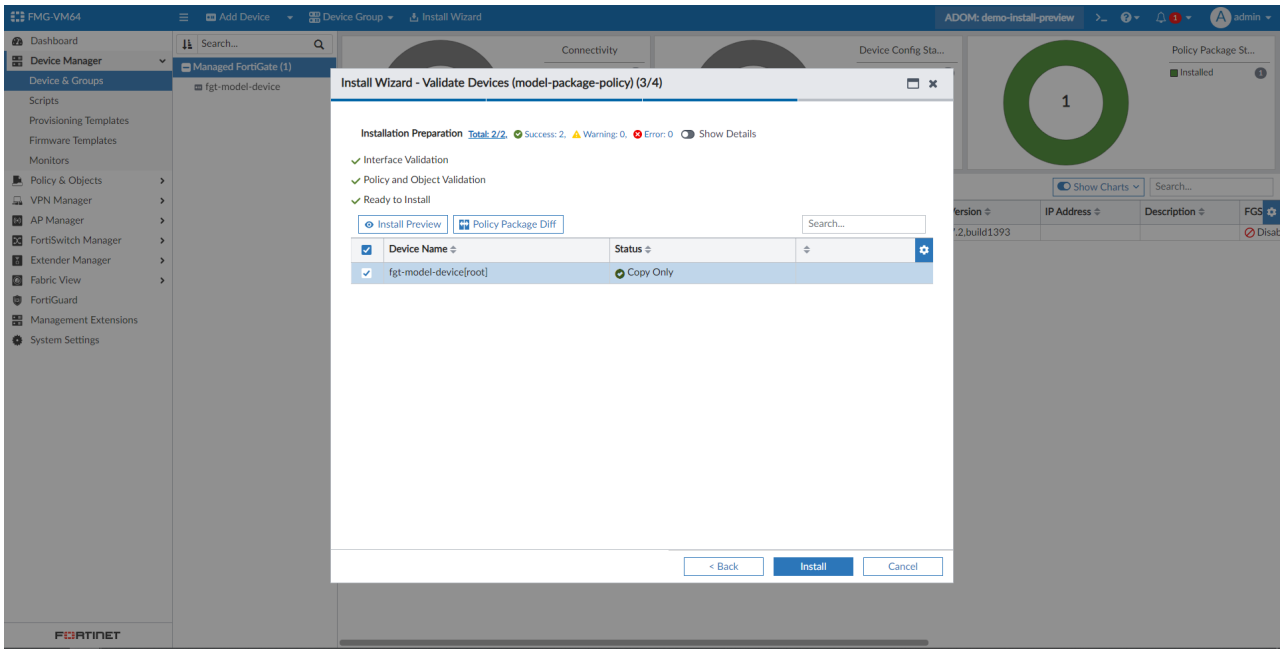
3. Launch *Install Wizard*. Select *Install Policy Package & Device Settings*. Choose the *Policy Package* and click *Next*.



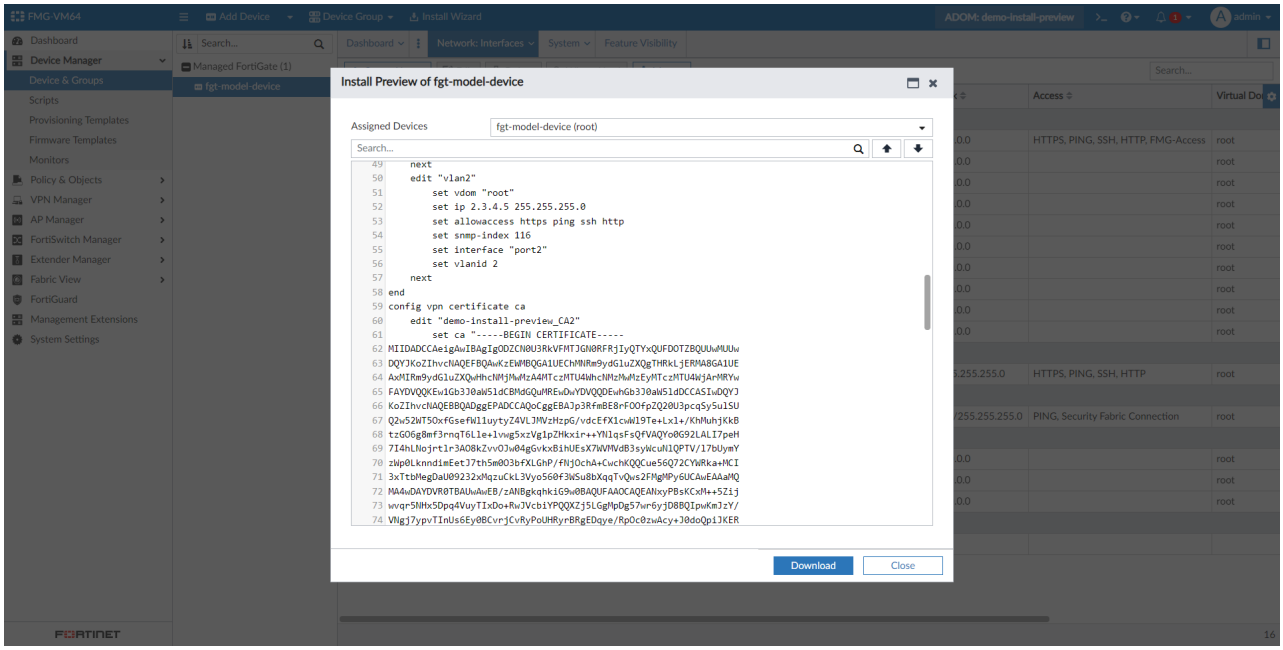
4. Select the target model device and click *Next*.



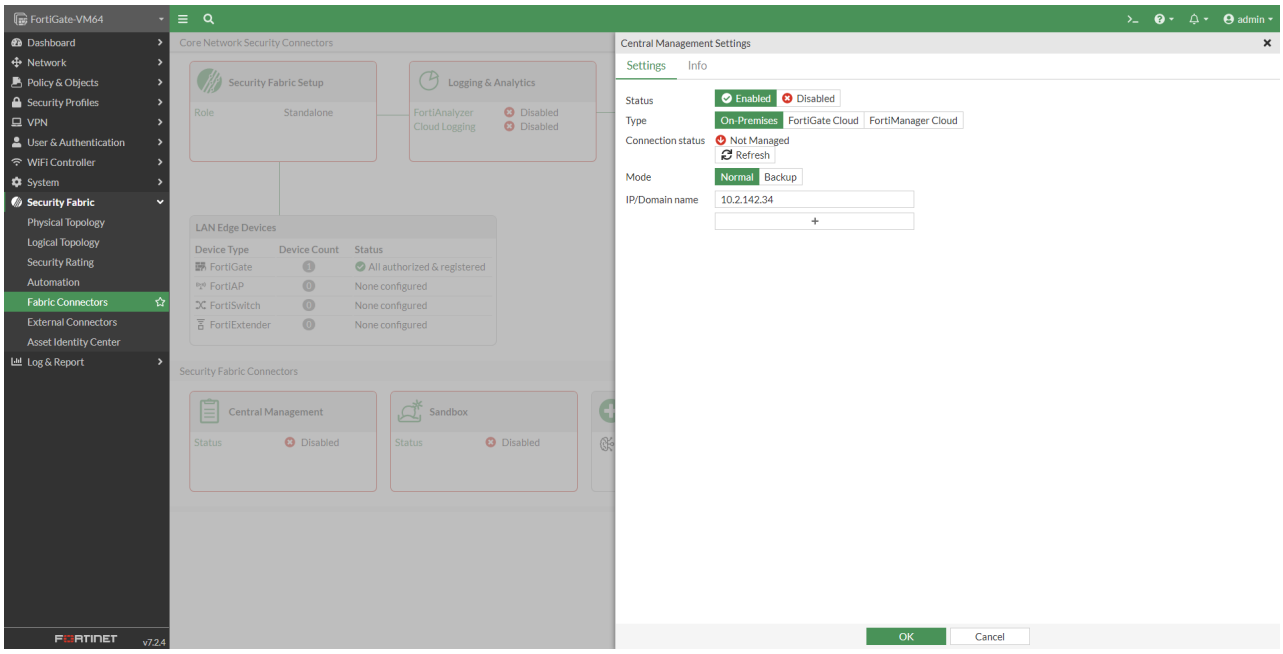
5. Click *Install Preview*.



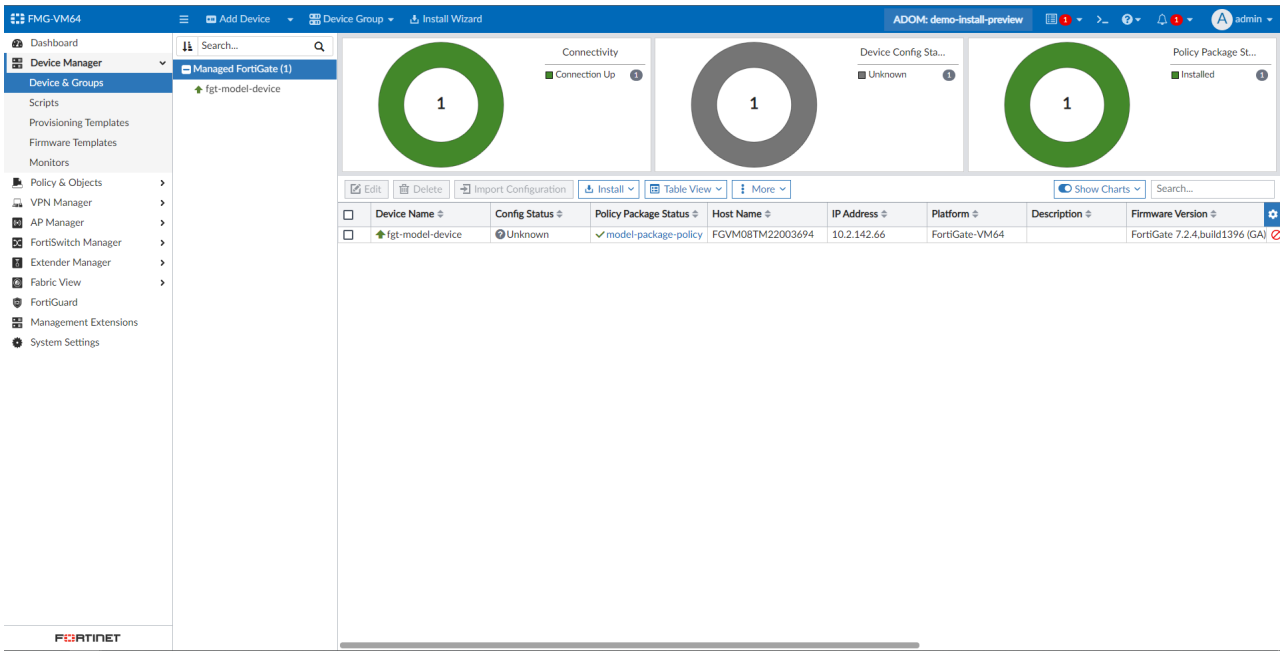
6. In the configuration that is displayed, scroll down to view the new configuration in the system interface table. Use this preview to verify that the new interface is created and is being installed to the model device correctly.



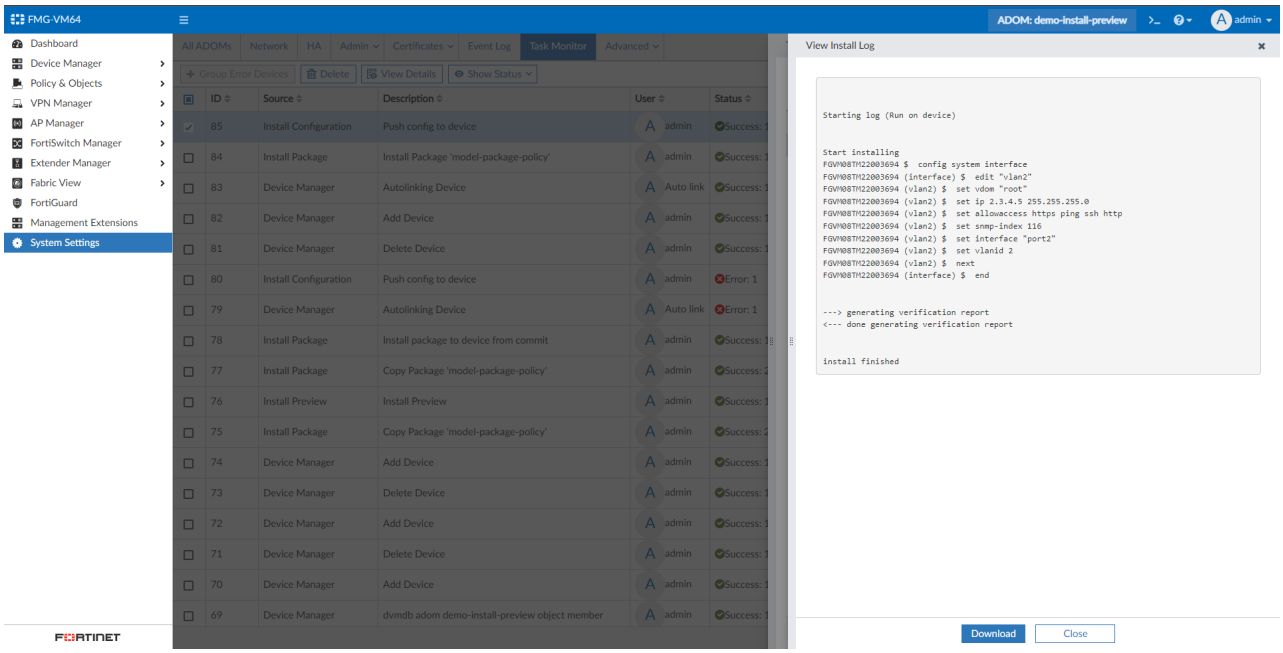
7. Connect the FortiGate to FortiManager to initiate autolink and push the configuration changes.



8. Verify that the device status is changed to *Online*.



9. From *Task Monitor*, view the install log to verify the change is being pushed to the device successfully.



Some configurations that originally exist in a real device could significantly impact the accuracy of the install preview during an autolink operation.

Examples of these configurations include:

- Hardware specifications.
- Firmware versions and builds.
- Overlapping configurations.

VPN Monitoring displays IPsec VPN tunnels created by IPsec templates and SD-WAN overlay wizard

This information is also available in the FortiManager 7.4 Administration Guide:

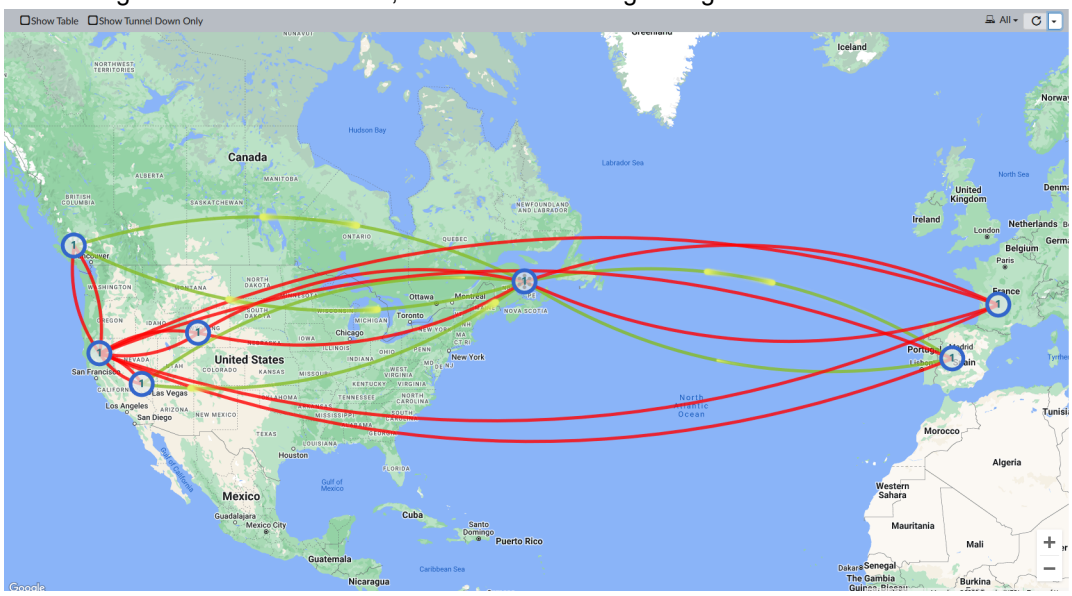
- VPN Monitor

VPN Monitoring displays IPSec VPN tunnels created by IPsec Templates and the SD-WAN Overlay Wizard with specific device icon identification for HUBs and the ability to drilldown to a device group level.

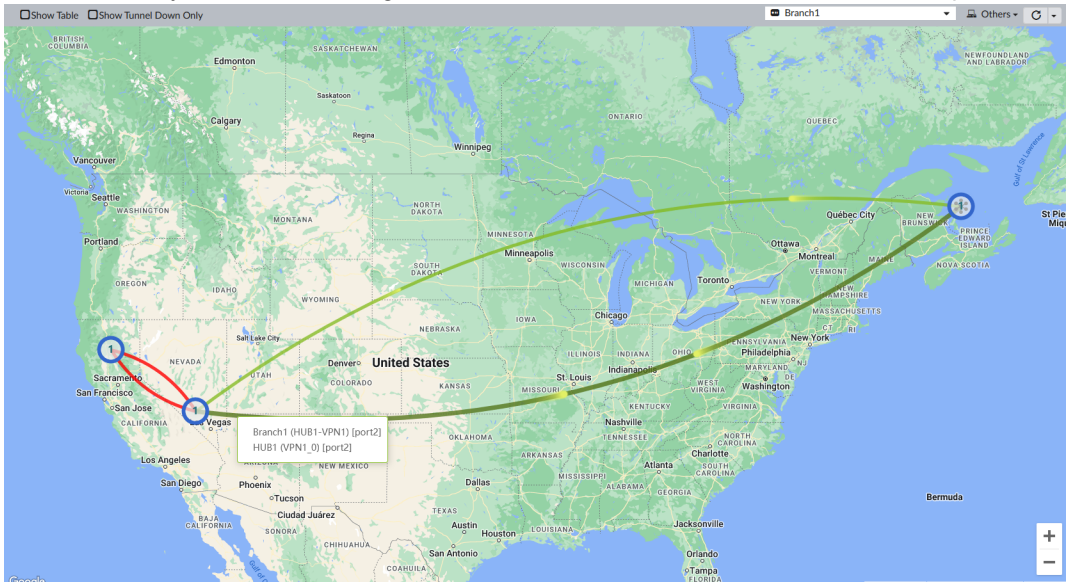
To view IPsec tunnel template information in the VPN Monitor:

1. Go to *Device Manager* > *Monitors* > *VPN Monitor*.
   The VPN Monitor displays all IPsec VPN tunnel information created with the VPN Manager, IPsec template, or created directly on FortiOS.

2. The map includes the following information:
   - Green lines indicate that a tunnel is up.
     - When the green lines are animated, there is traffic flowing through the VPN tunnels.

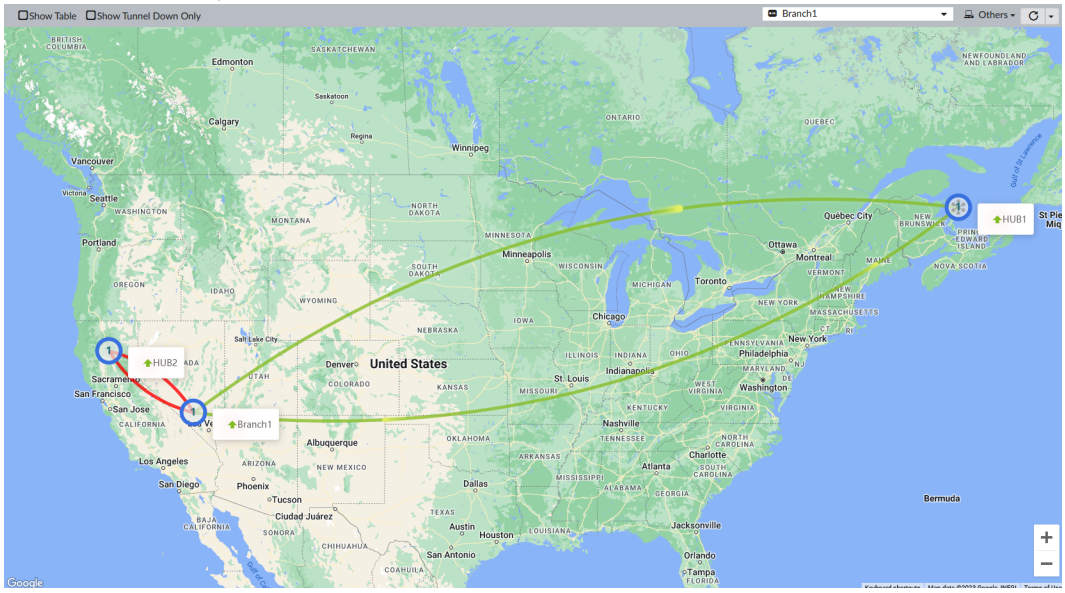


     - You can hover your mouse over a green line to view the VPN tunnel name and source port information.

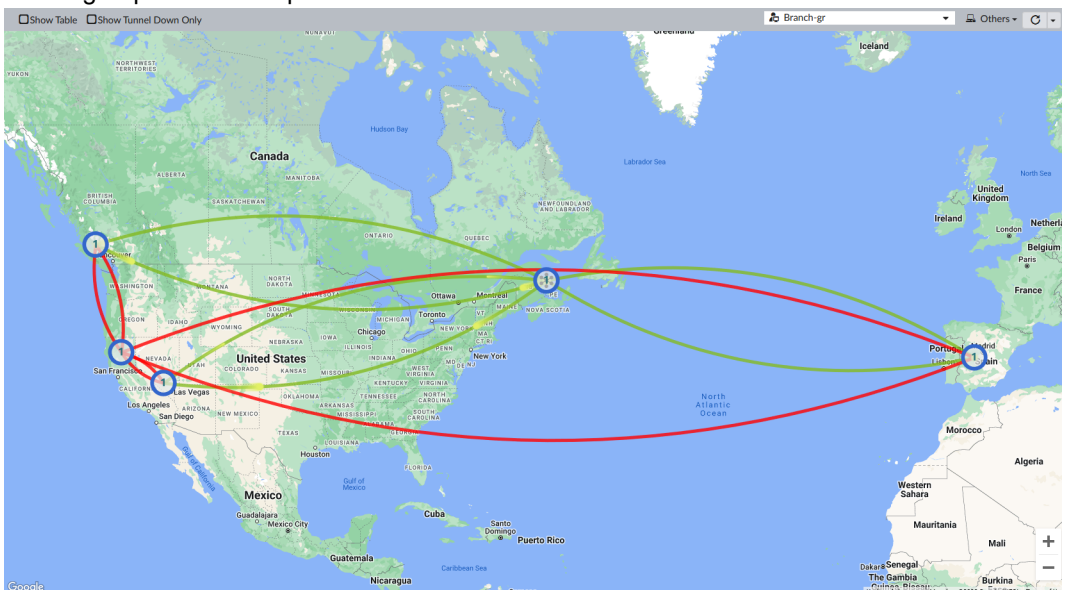


   - Red lines indicate that a tunnel is down.
   - HUB device(s) are identified with a star icon.

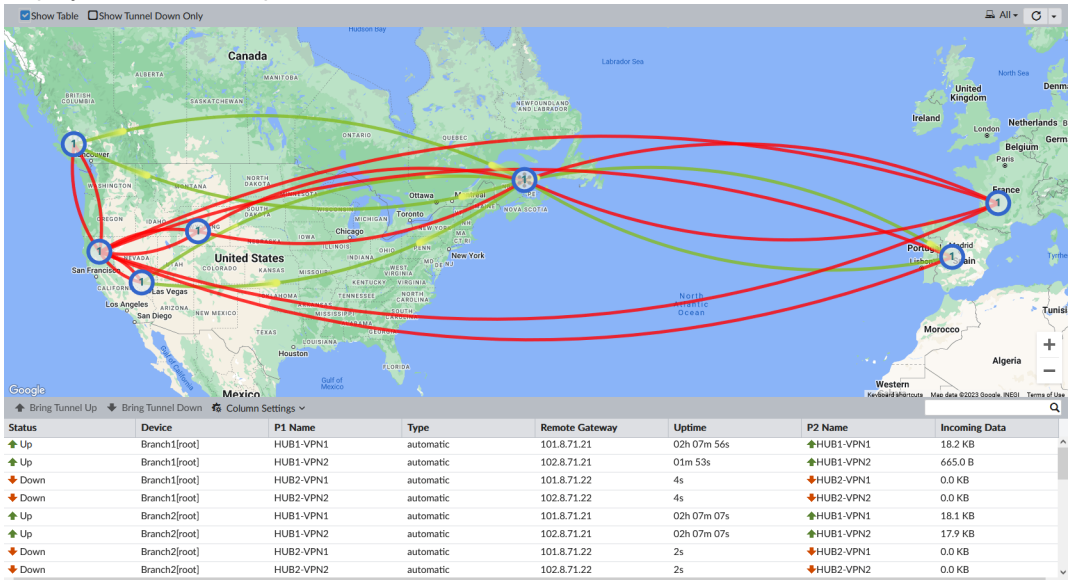
3. To view a single device's IPsec VPN tunnel information, change *All* to *Others* in the toolbar menu, and select a device from the dropdown.



4. To view a device group's IPsec VPN tunnel information, change *All* to *Others* in the toolbar menu, and select a device group from the dropdown.



5. To view IPsec VPN tunnel information in a table, select the *Show Table* option from the toolbar and the table will be displayed under the map.



Status	Device	P1 Name	Type	Remote Gateway	Uptime	P2 Name	Incoming Data
Up	Branch1[root]	HUB1-VPN1	automatic	101.8.71.21	02h 07m 56s	HUB1-VPN1	18.2 KB
Up	Branch1[root]	HUB1-VPN2	automatic	102.8.71.21	01m 53s	HUB1-VPN2	665.0 B
Down	Branch1[root]	HUB2-VPN1	automatic	101.8.71.22	4s	HUB2-VPN1	0.0 KB
Down	Branch1[root]	HUB2-VPN2	automatic	102.8.71.22	4s	HUB2-VPN2	0.0 KB
Up	Branch2[root]	HUB1-VPN1	automatic	101.8.71.21	02h 07m 07s	HUB1-VPN1	18.1 KB
Up	Branch2[root]	HUB1-VPN2	automatic	102.8.71.21	02h 07m 07s	HUB1-VPN2	17.9 KB
Down	Branch2[root]	HUB2-VPN1	automatic	101.8.71.22	2s	HUB2-VPN1	0.0 KB
Down	Branch2[root]	HUB2-VPN2	automatic	102.8.71.22	2s	HUB2-VPN2	0.0 KB

FortiManager supports CLI diff in the workflow approval sessions

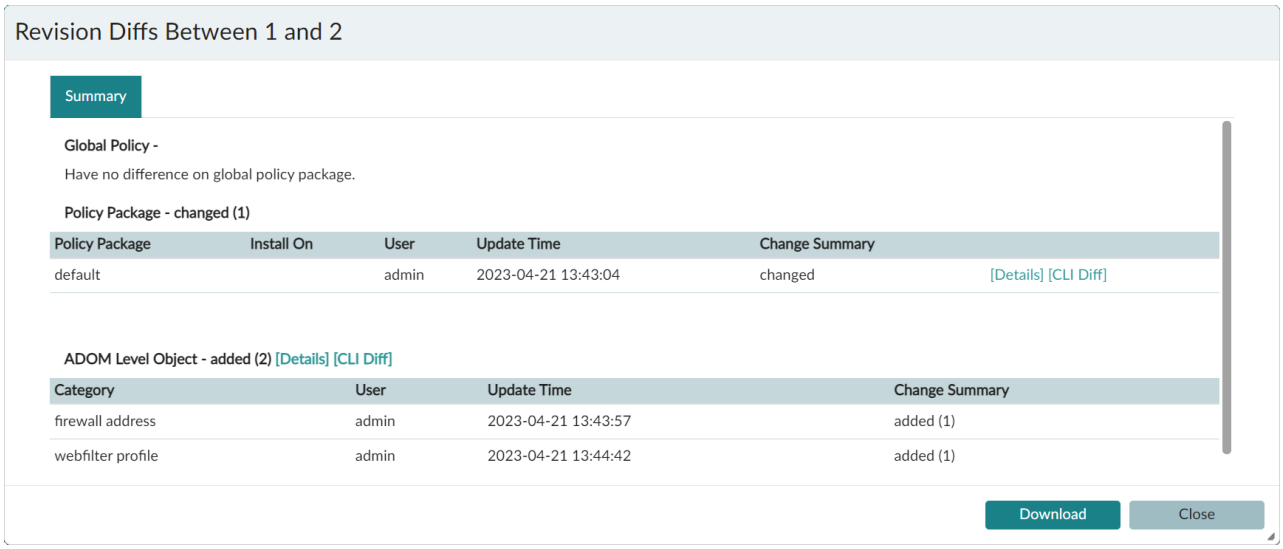
This information is also available in the FortiManager 7.4 Administration Guide:

- View session diff

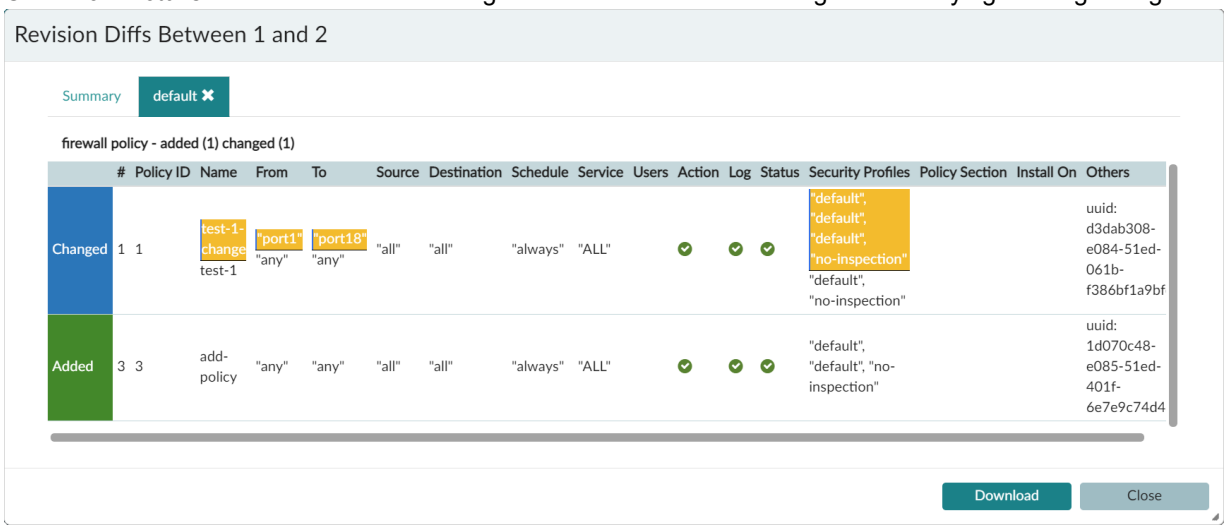
FortiManager supports CLI diff in the workflow approval sessions.

To view the CLI diff in workflow approvals:

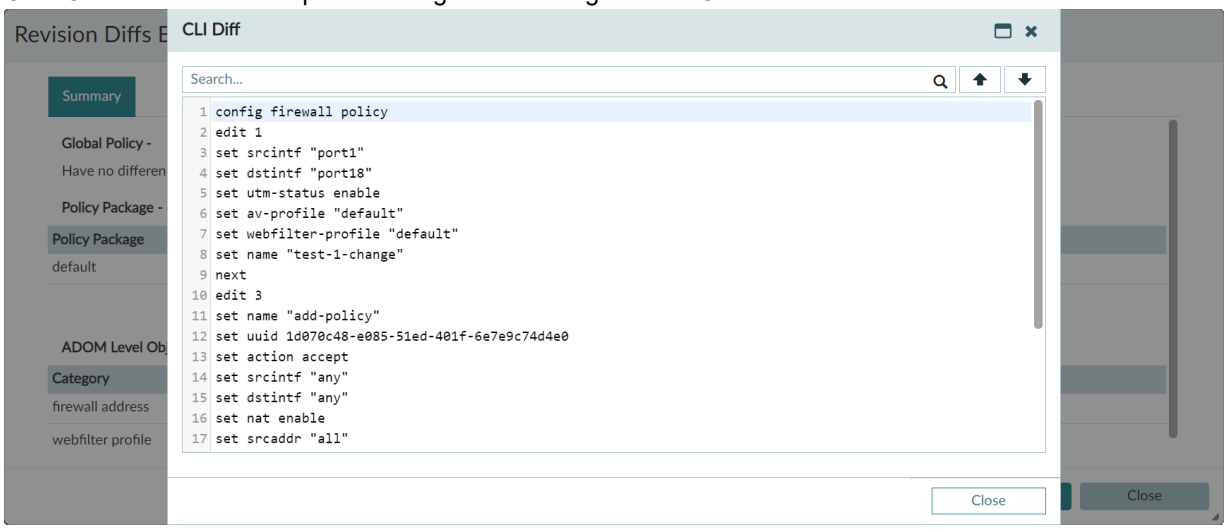
1. In *Workflow* mode, create a session and make some changes.
2. Save the changes, and click *View Diff*.
   The Revision Diffs dialog includes the new *CLI Diff* option.



- Click *View Details* to see details of the change and if entries are new changes or modifying existing changes.



- Click *CLI Diff* to see more specific configuration changes in the CLI.



Internet Service database update occurs only if specific policy objects require a FortiGuard update - 7.4.1

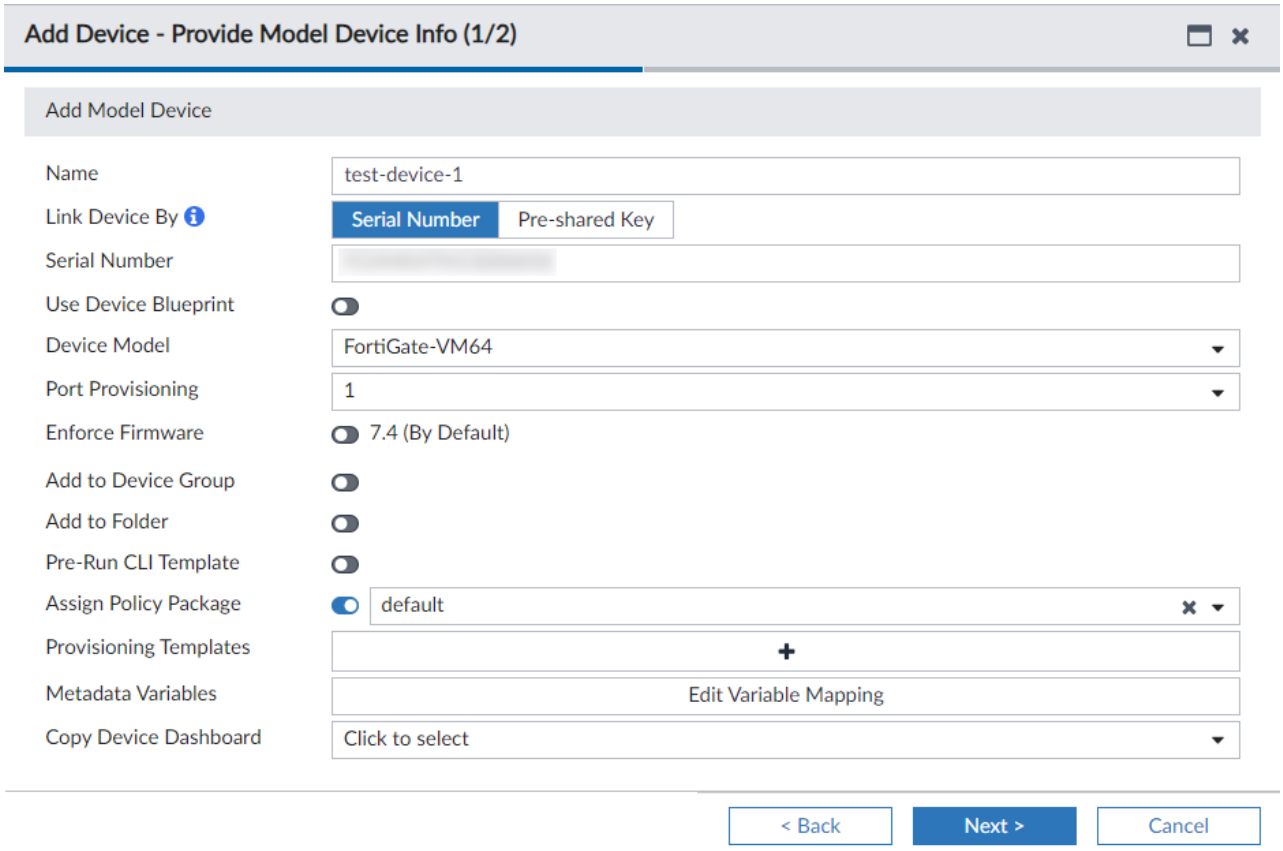
This information is also available in the FortiManager 7.4 Administration Guide:

- Adding offline model devices

ZTP process has been optimized with Internet Service database update occurring only if specific objects used in the policy require a FortiGuard update.

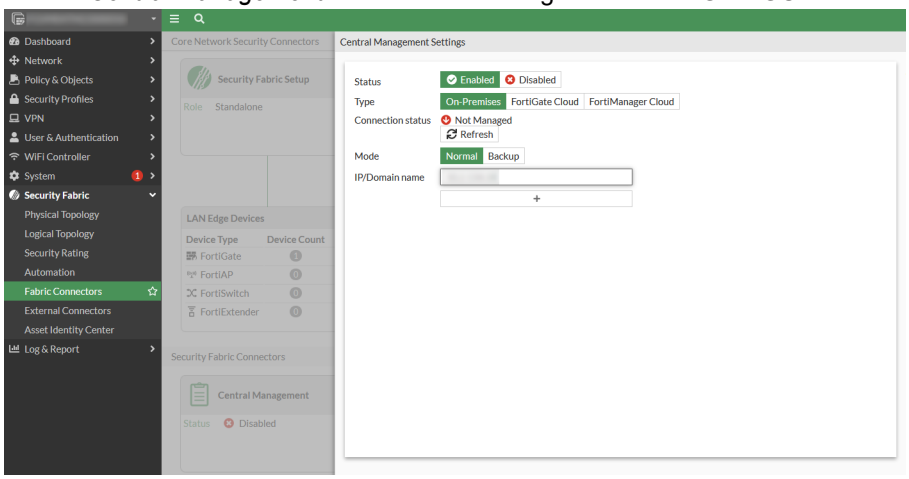
To see when an ISDB update will be performed:

1. On FortiManager, go to the *Device Manager* and add a model device.

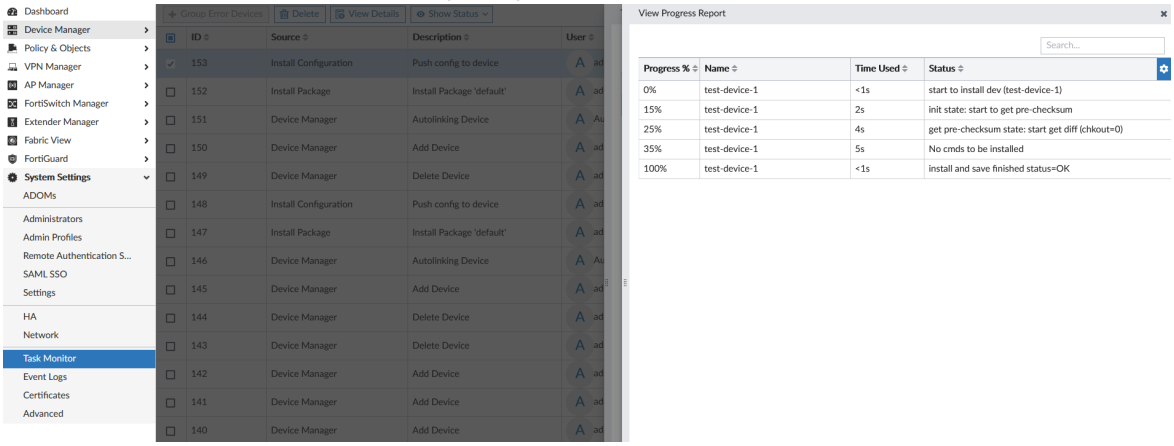


2. Assign a Policy Package to the device.

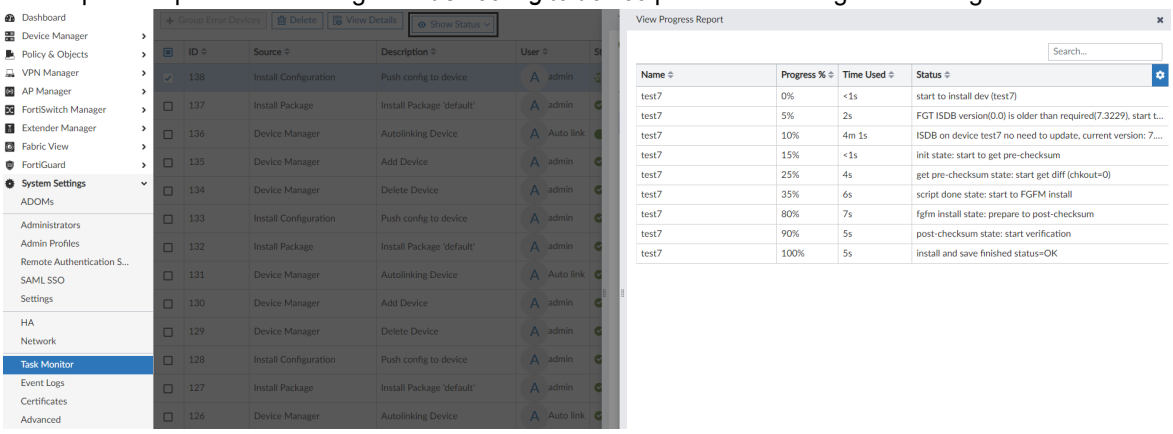
3. Enable *Central Management* from the FortiManager in the FortiGate GUI.



4. Following the device auto-link process, when the configuration is pushed to FortiGate, FortiManager determines if an ISDB update is required:
   - **ISDB update not required**:
     - If there is no Internet Service used in the Policy Package, there will be no ISDB update performed.
     - If the Internet Service used in the Policy Package is the same version or an older version than the version on the FortiGate, there will be no ISDB update performed.



   - **ISDB update required**:
     - If the Internet Service used in the Policy Package is newer than the ISDB version on the FortiGate, an ISDB update is performed during the *Push config to device* process following auto-linking.



Policy and Objects

This section lists the new features added to FortiManager for policy and objects:

Policy

This section lists the new features added to FortiManager for policies:

Install preview support for partial install

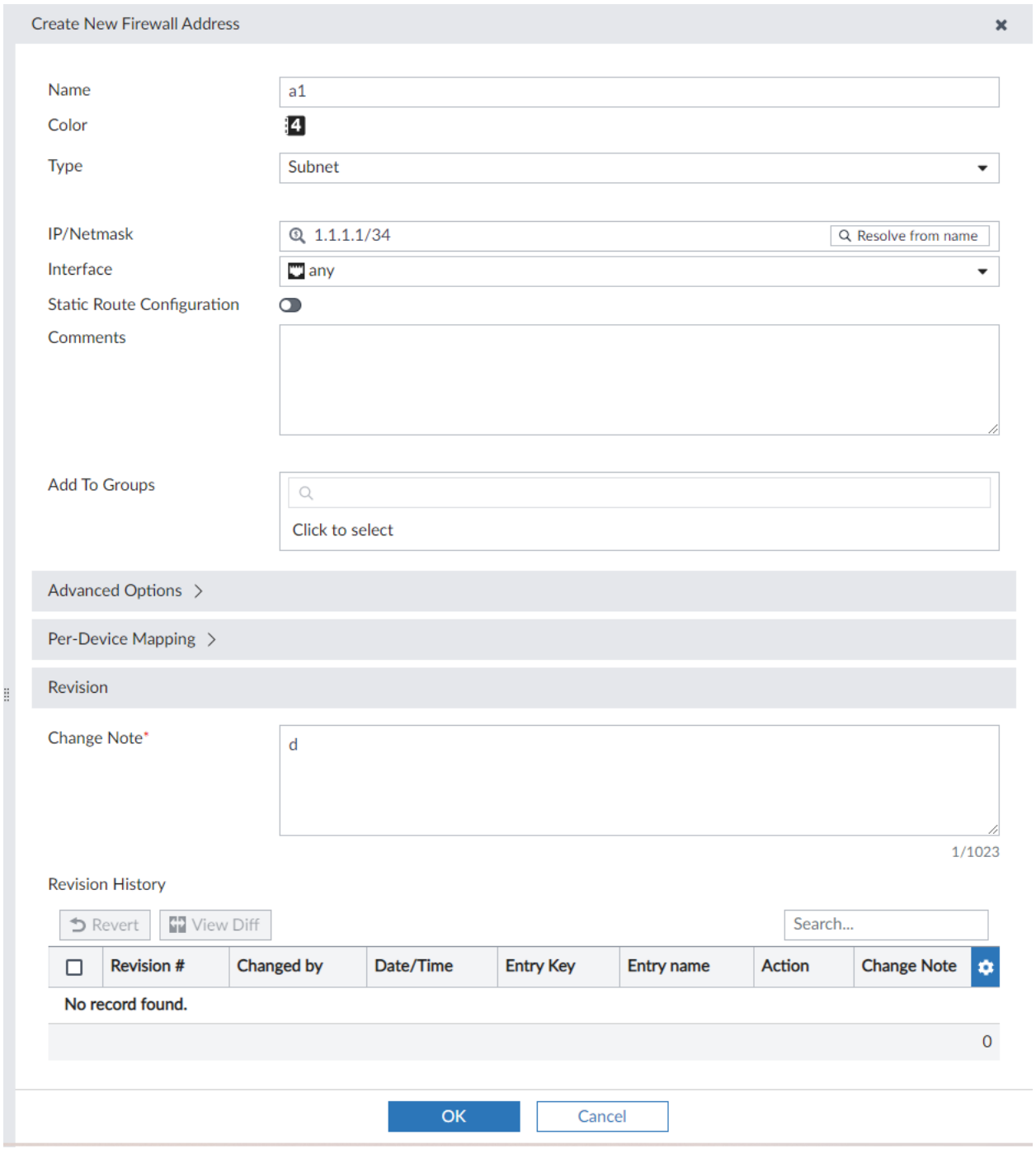
This information is also available in the FortiManager7.4 Administration Guide:

- Installing objects

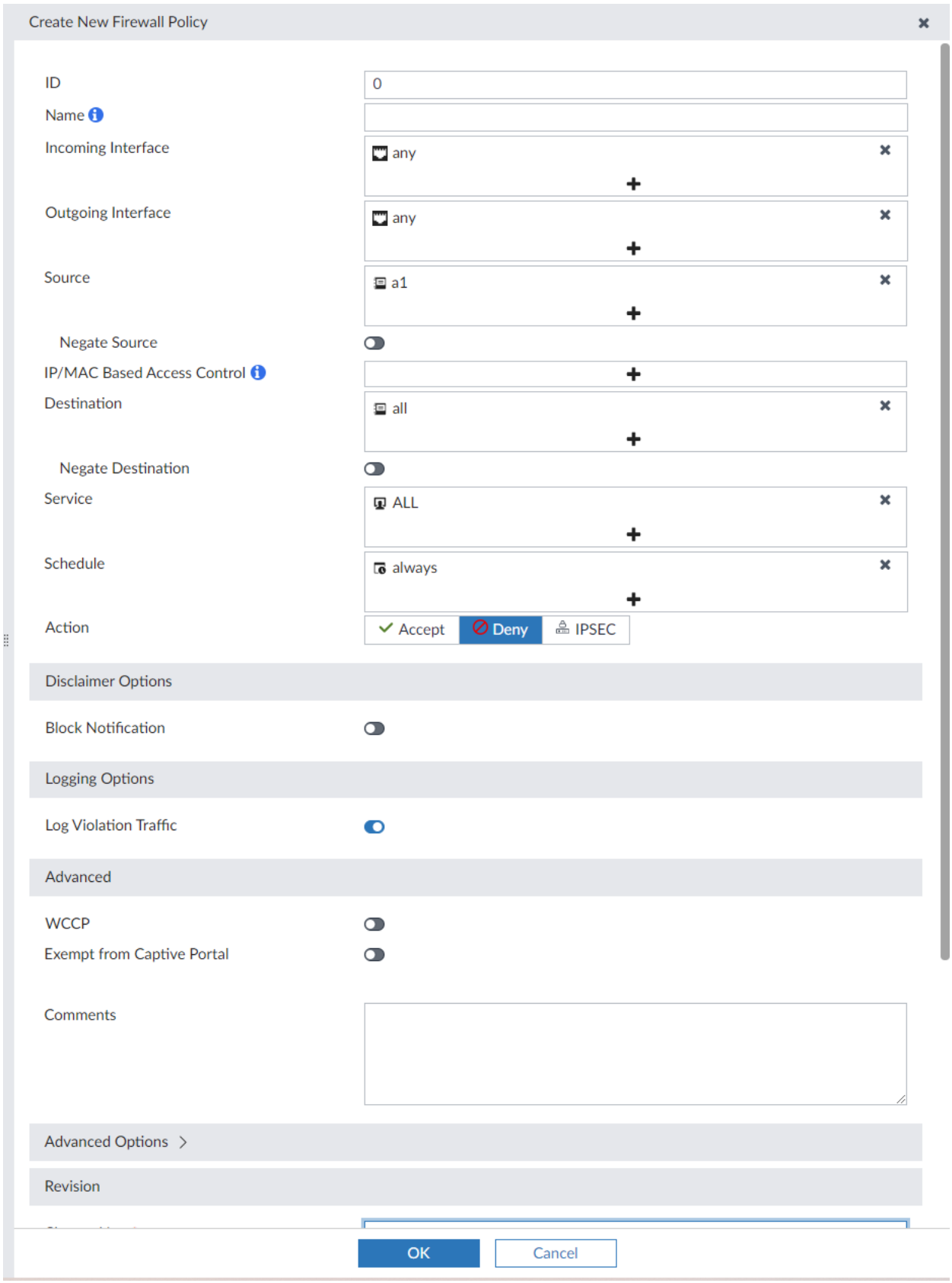
When the partial install feature is enabled, *Install Preview* can be used to view the configuration changes that will be made before a partial install.

To preview a partial install:

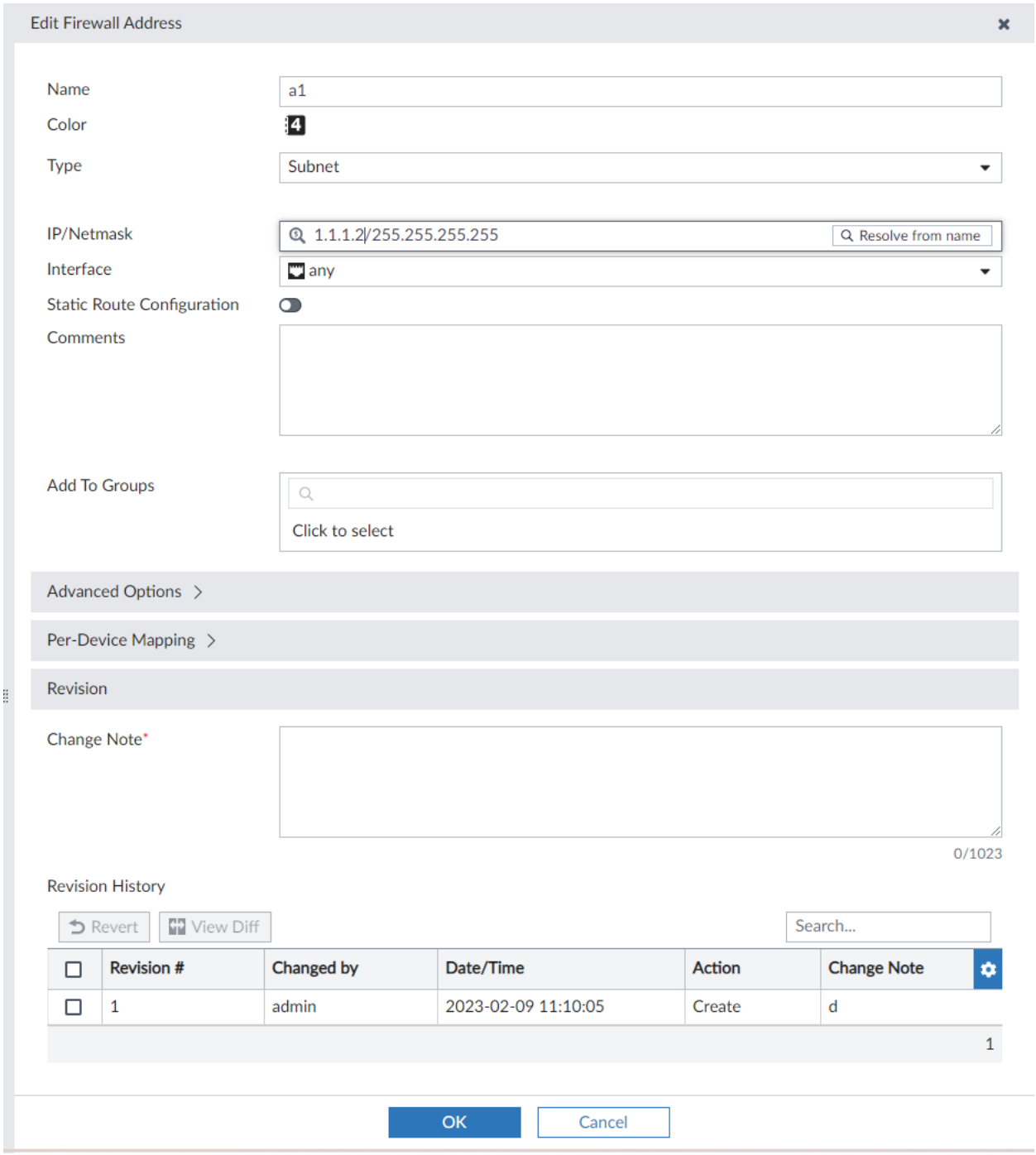
1. In the FortiManager CLI, enable partial install:
```
config system global
   set partial-install enable
end
```
2. Create an address `a1`.



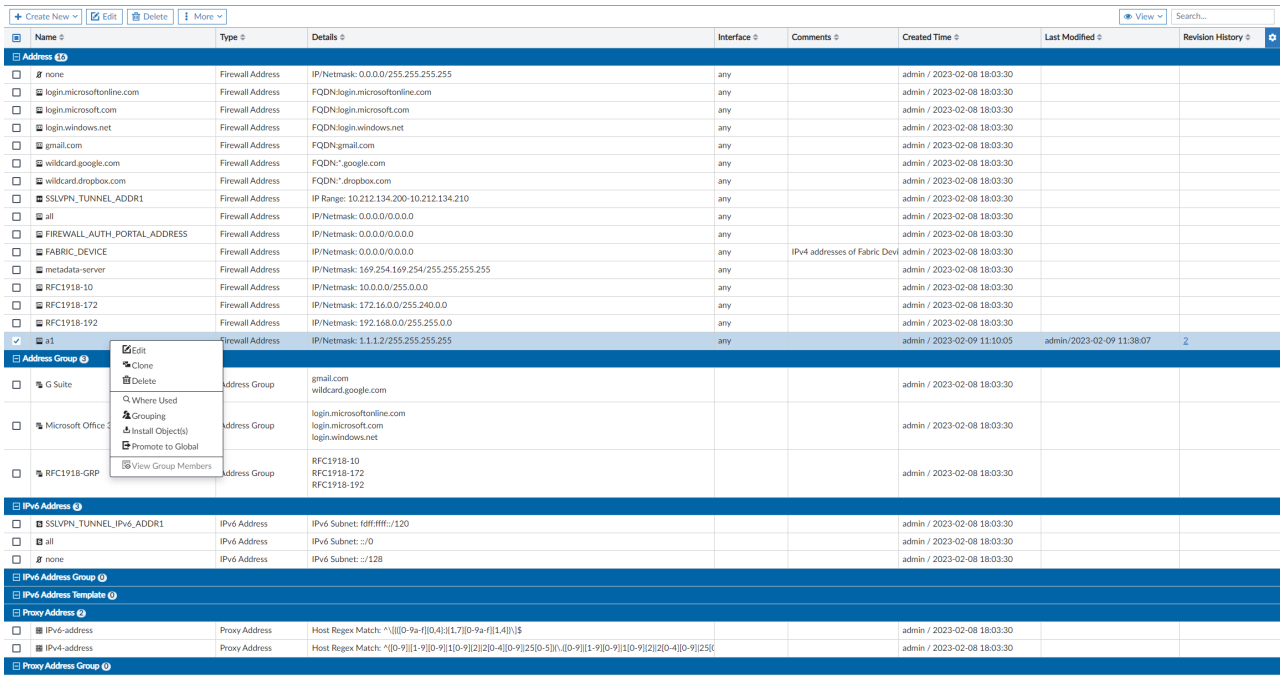
3. Use this address in a policy.


Create New Firewall Policy
ID
0
Name
Incoming Interface
any
Outgoing Interface
any
Source
a1
Negate Source
IP/MAC Based Access Control
Destination
all
Negate Destination
Service
ALL
Schedule
always
Action
Accept
Deny
IPSEC
Disclaimer Options
Block Notification
Logging Options
Log Violation Traffic
Advanced
WCCP
Exempt from Captive Portal
Comments
Advanced Options
Revision
OK
Cancel

4. Install the policy to a FortiGate.
5. Modify the `a1` address.



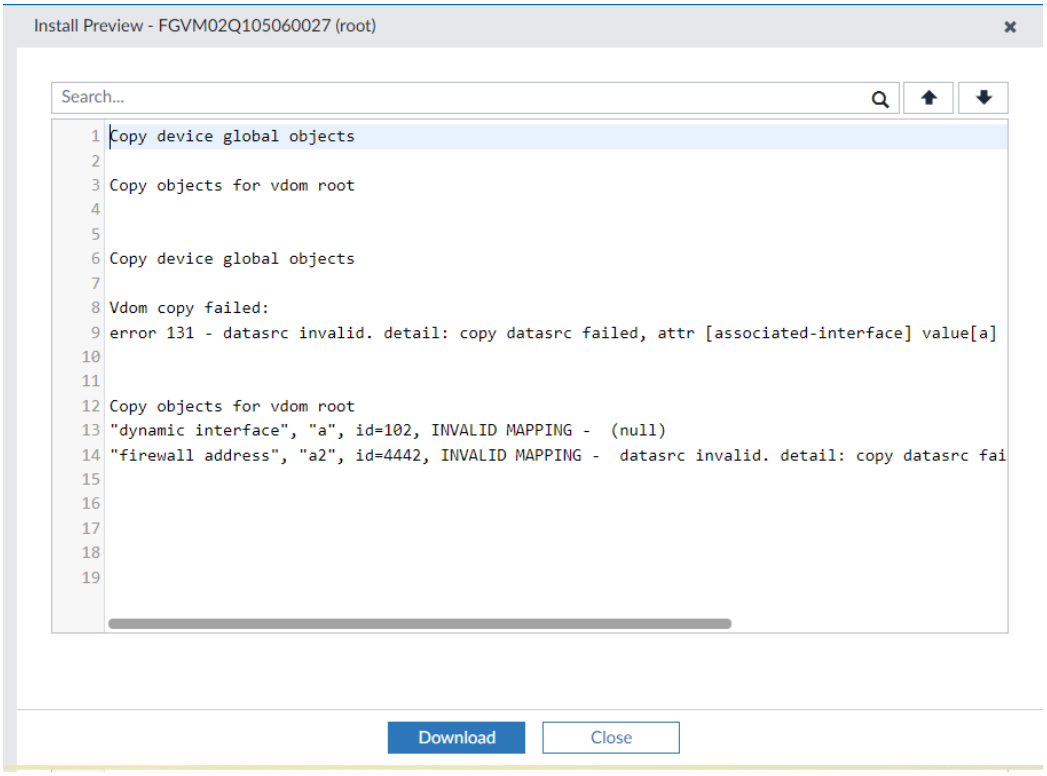
6. Right click `a1` and select *Install Object(s)*.



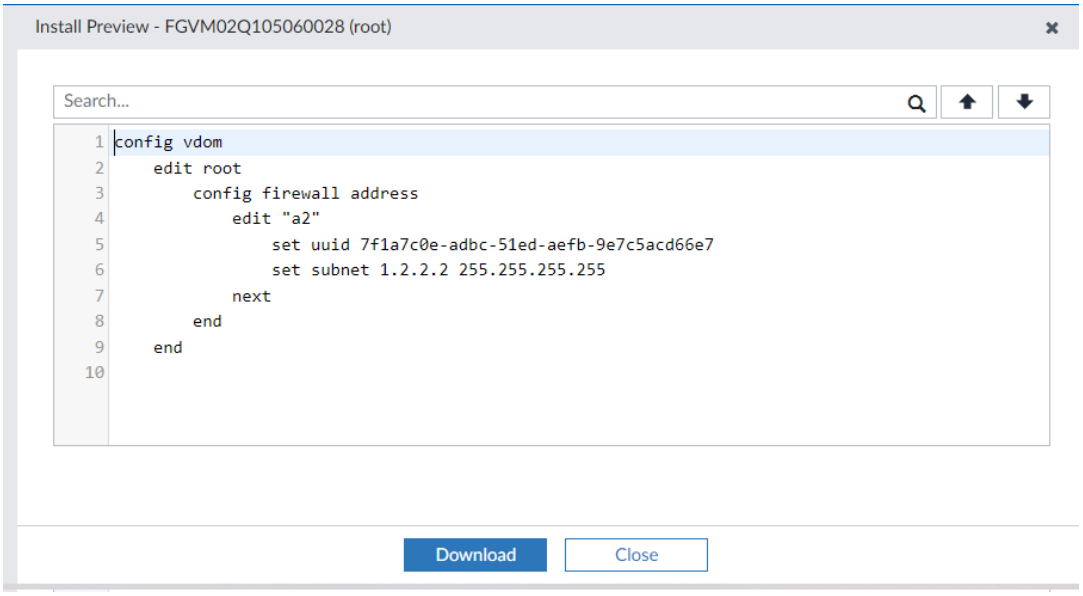
7. Select the installation target and click *Install Preview*.
8. The install preview displays the pending configuration changes.

If you attempt to install an object that is not used in a policy, the device list displays *No record found*.

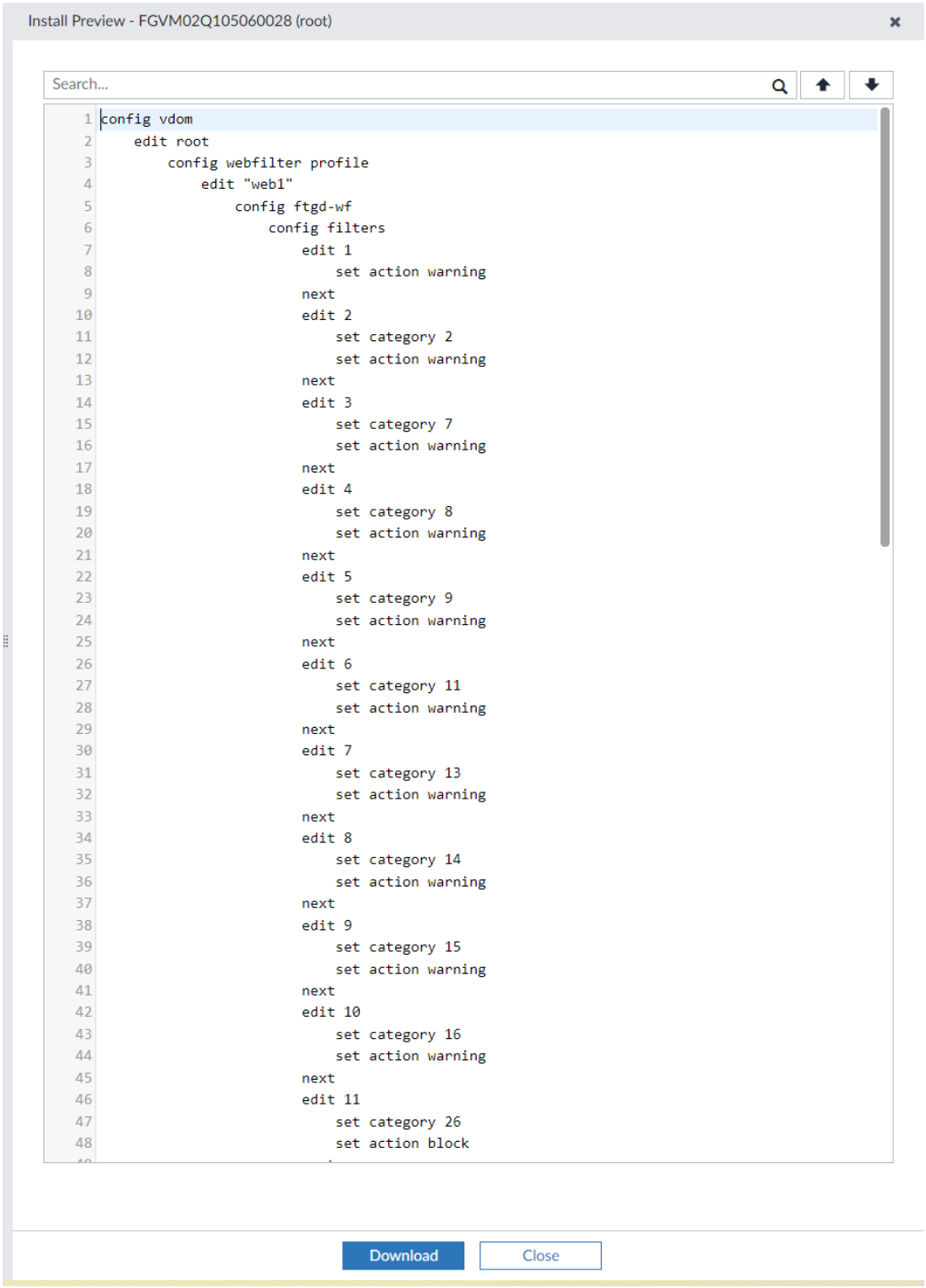
If you attempt to install an object with invalid configuration, *Install Preview* displays the configuration errors.



In *Install Preview*, metadata variables used in objects display the real value.



Administrators with a restricted profile can use *Install Preview* for partial installs.



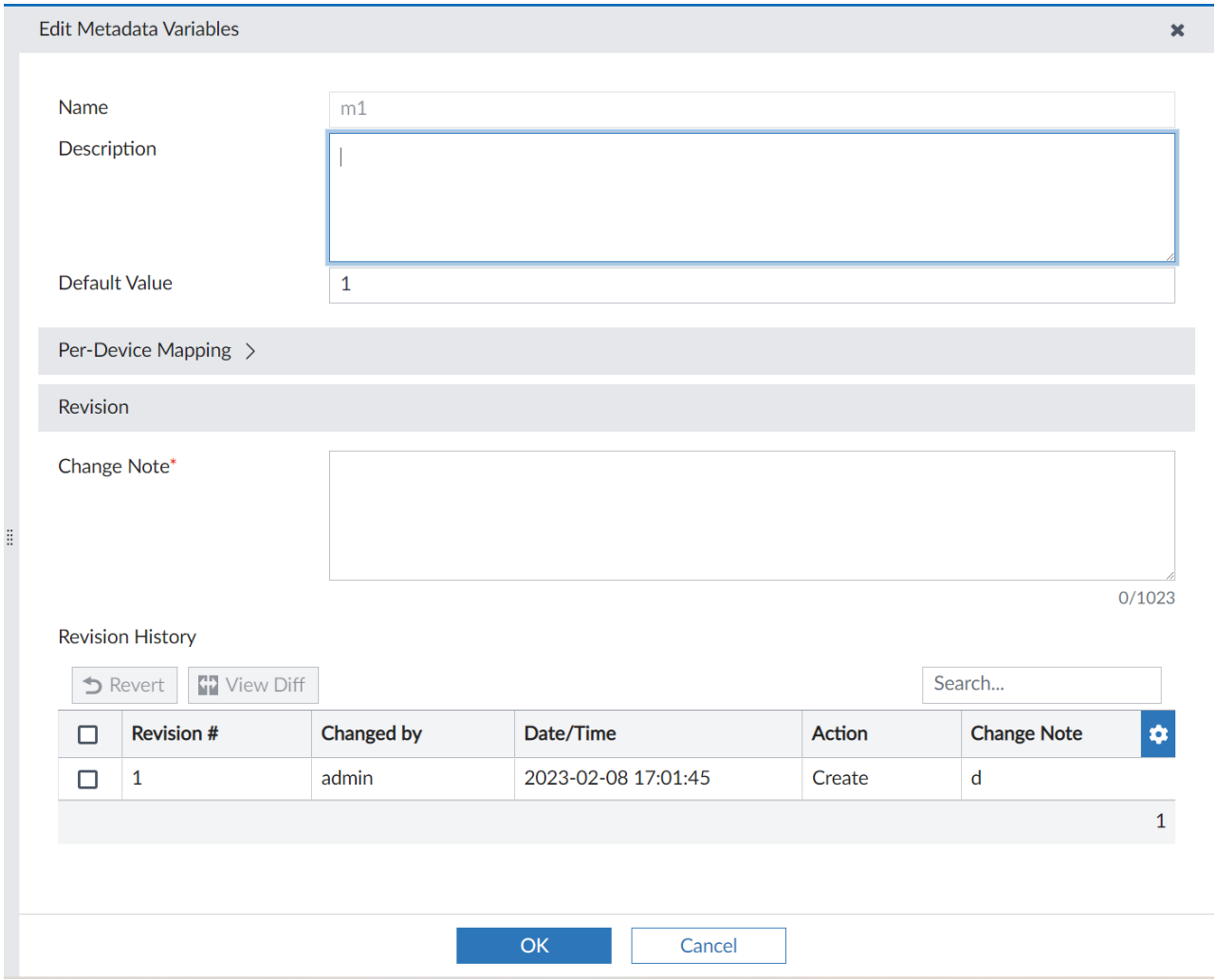
Policy Package installation added link to the progress report page for installation errors

This information is also available in the FortiManager7.4 Administration Guide:
- Installing policy packages and device settings

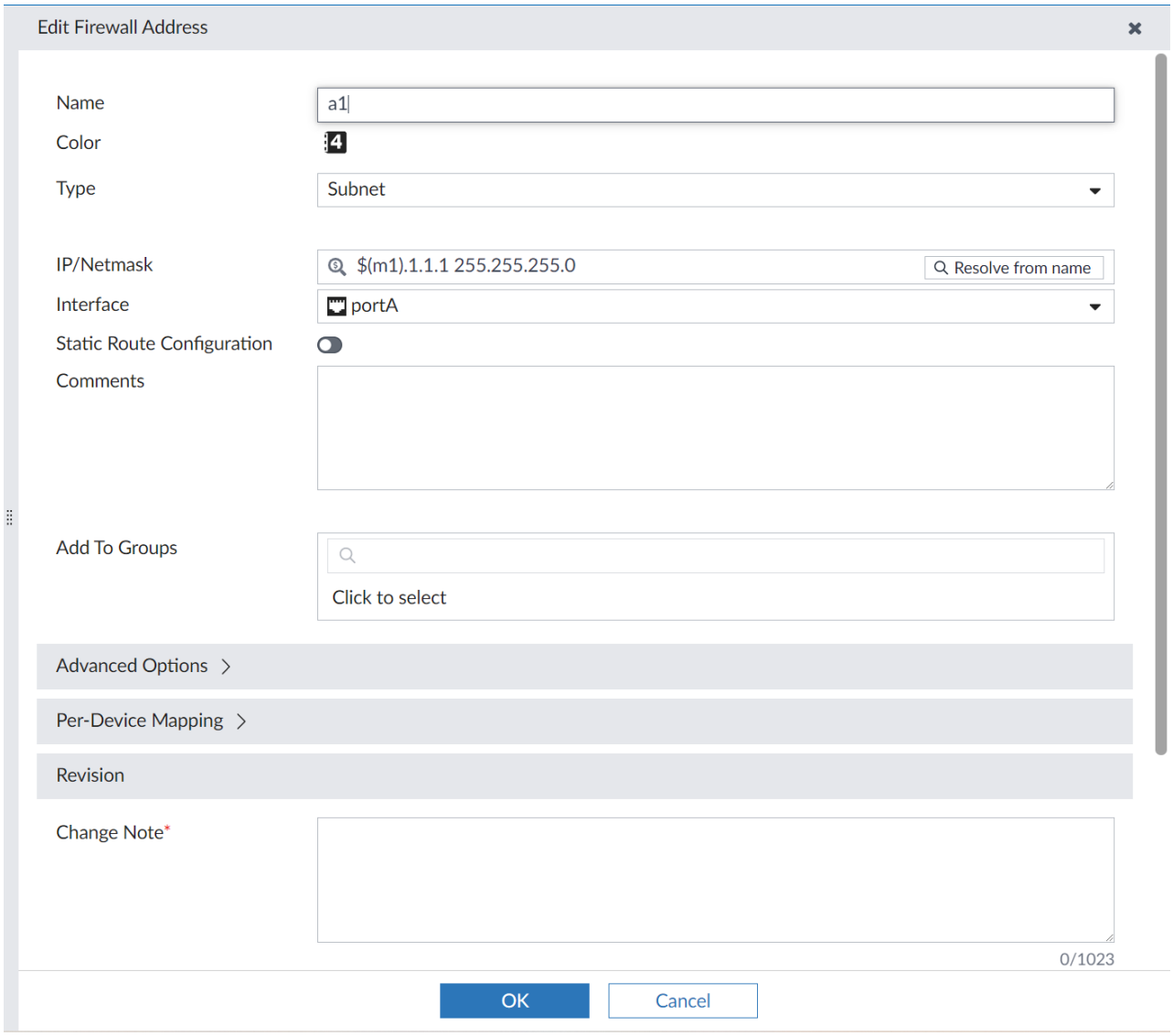
When there is an error in policy and settings validation, you can view the progress report to see the specific error that occured.

To view the progress report in the case of an install error:

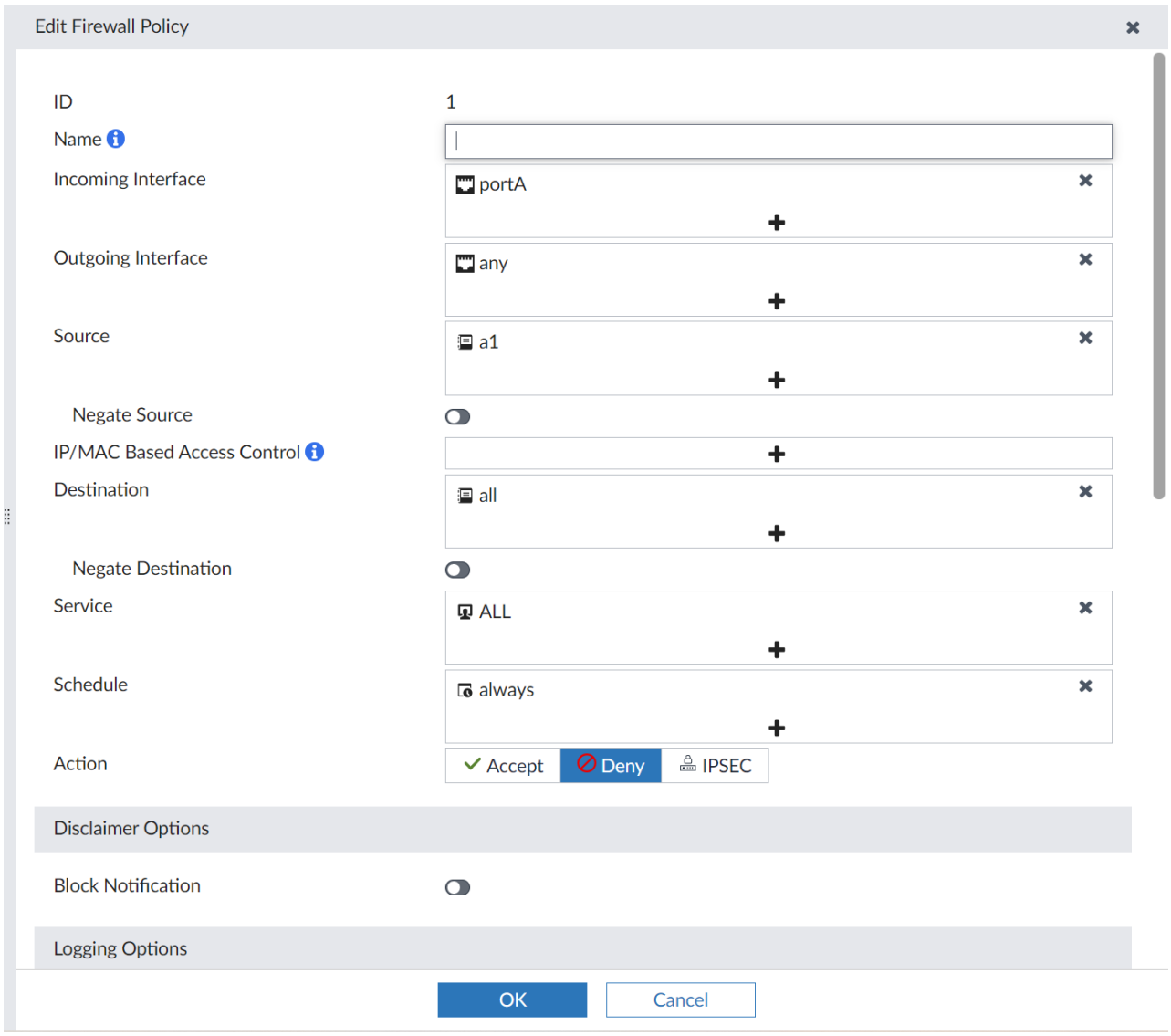
1. Create a metadata variable `m1` with a default value of `1`.



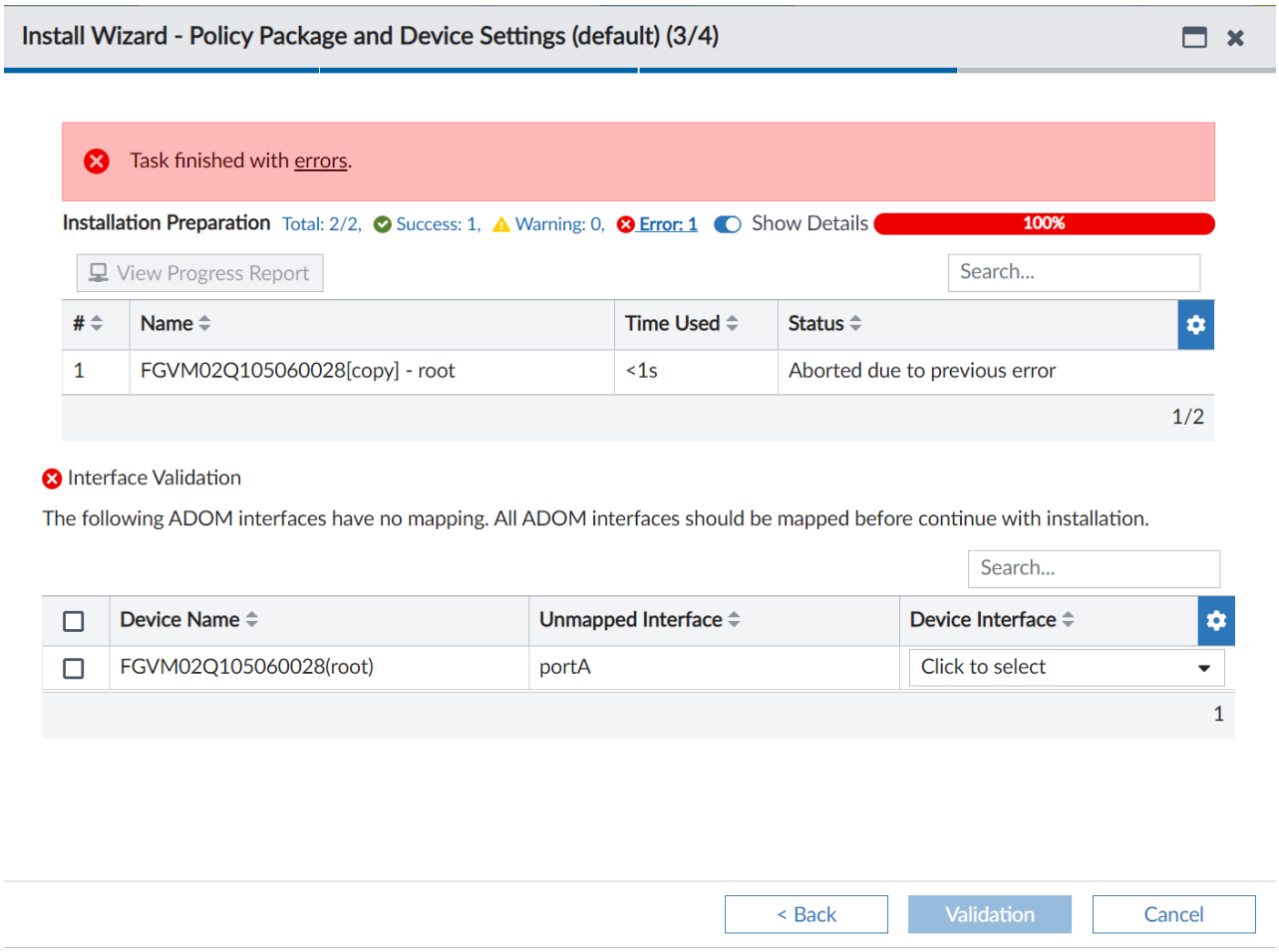
2. Create an address `a1` using the new metadata variable `m1` in it and bind the address to *portA*.



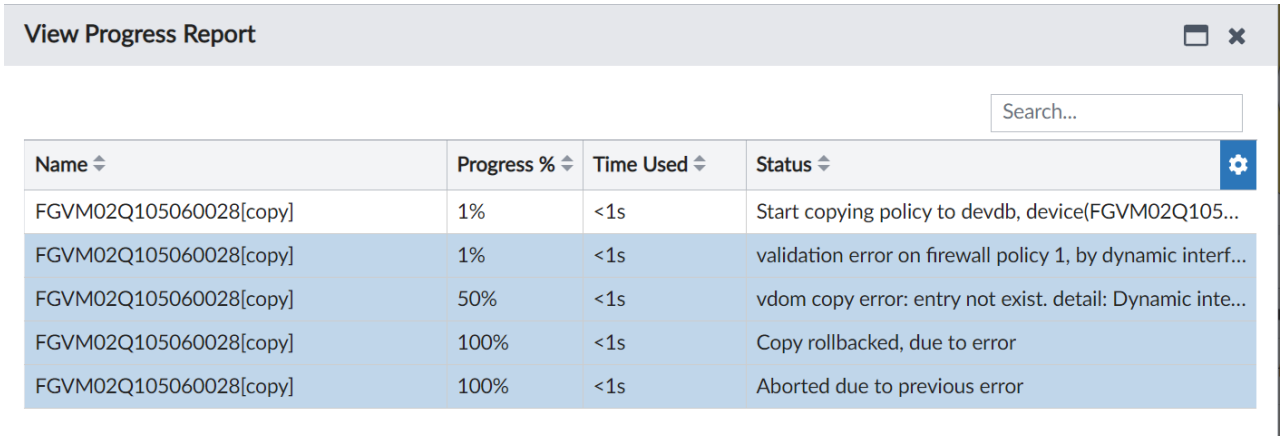
3. Create a policy with *Source* set to `a1` and *Incoming Interface* set to *portA*.



4. Launch *Install Wizard*. Select *Install Policy Package & Device Settings* and continue to the validation step.
   The *Install Wizard* displays an error message.



5. In the error message, click on *errors*.
   The progress report displays with the error lines highlighted.



Triple-click on a *Status* message to copy it and paste it to another document to read the full message.

Support for IoT Virtual Patching in NAC policies using pre-built severity filters

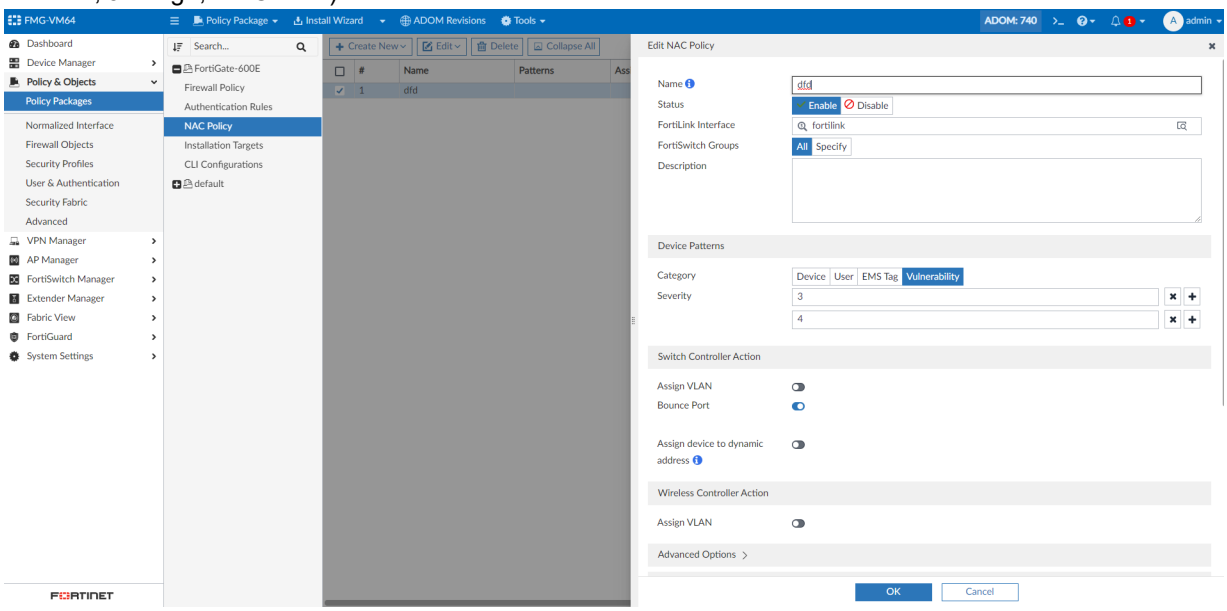
FortiManager includes support for IoT Virtual Patching in NAC policies using pre-built severity filters.

This information is also available in the FortiManager 7.4 Administration Guide:

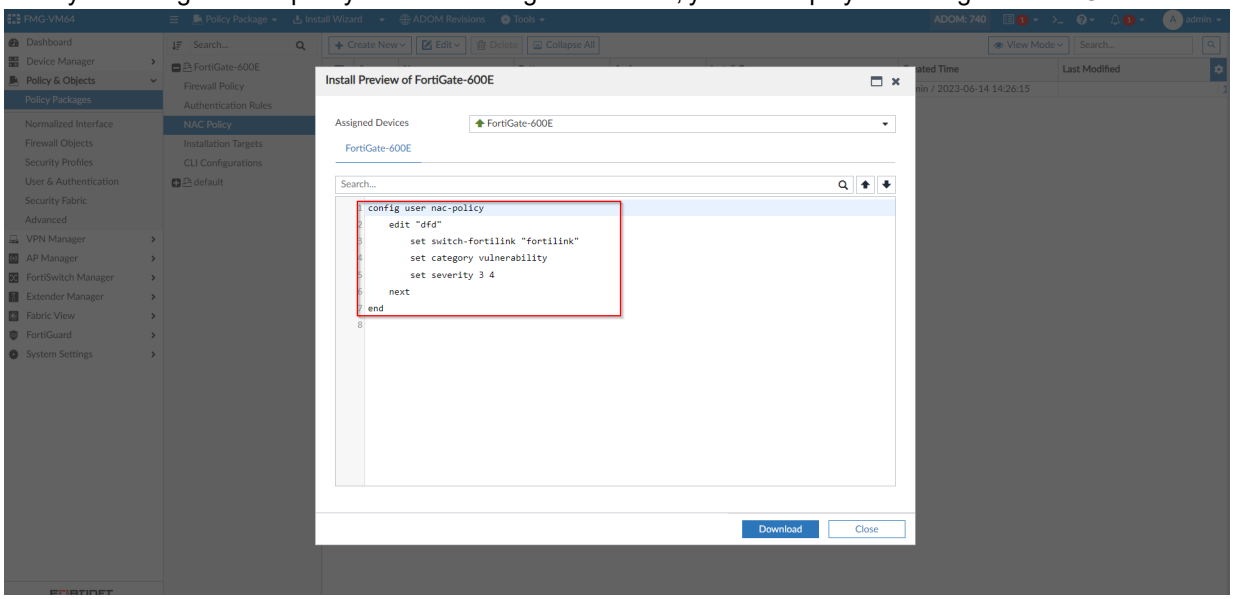
- Create a new NAC policy

To use IoT Virtual Patching in a NAC policy:

1. Go to *Policy & Objects* > *Policy Packages*, and create a new *NAC Policy*.
2. In the policy settings, select the *Vulnerability* category, then specify the *Severity* value (0 = Info, 1 = Low, 2 = Medium, 3 = High, 4 = Critical).



3. Save your changes to the policy. After the changes are made, you can deploy the changes to FortiGate.



Policy deletion warning message improved with selected policy number and name reference - 7.4.1

This information is also available in the FortiManager 7.4 Administration Guide:

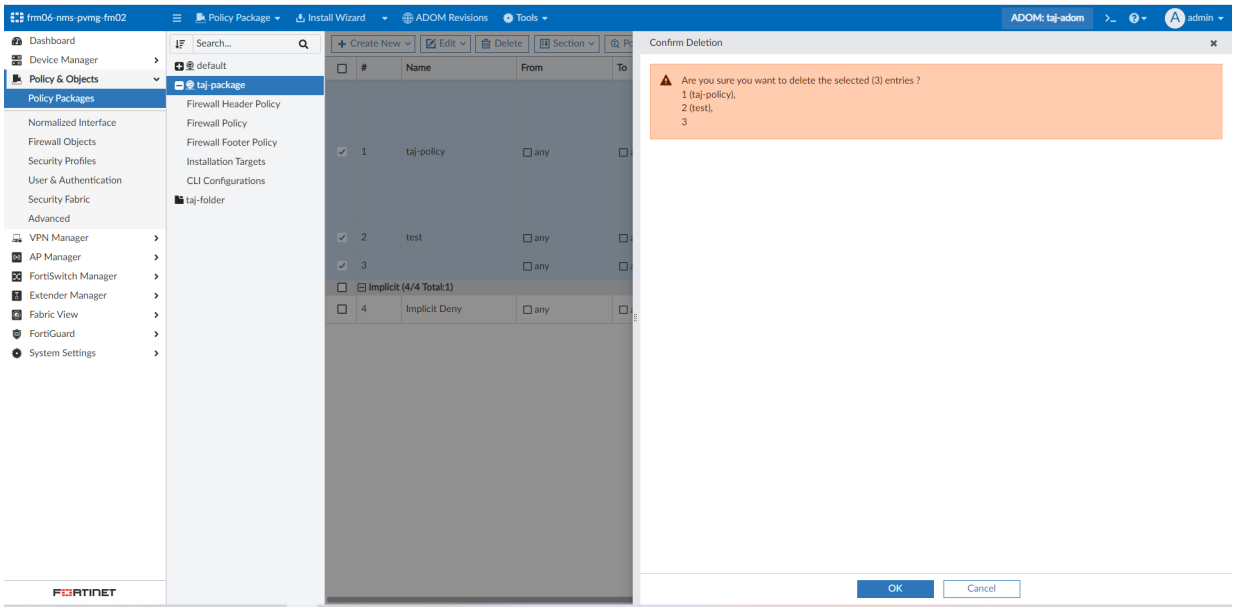
- Editing policies

In FortiManager, the policy deletion warning message is improved with the selected policy number and name reference.

To view the confirmation when deleting a policy:

1. Go to *Policy & Objects* > *Policy Packages*.

2. Select a policy, and click *Delete* in the toolbar.
   The *Confirm Deletion* pane displays information about the policies that will be deleted.



Enable option for persistent policy hit-count on ADOM database - 7.4.1

This information is also available in the FortiManager 7.4 Administration Guide:

- Policy hit count

In FortiManager 7.4.1, you can enable an option for a persistent policy hit-count on the ADOM database.

To save Last Used values on FortiManager:

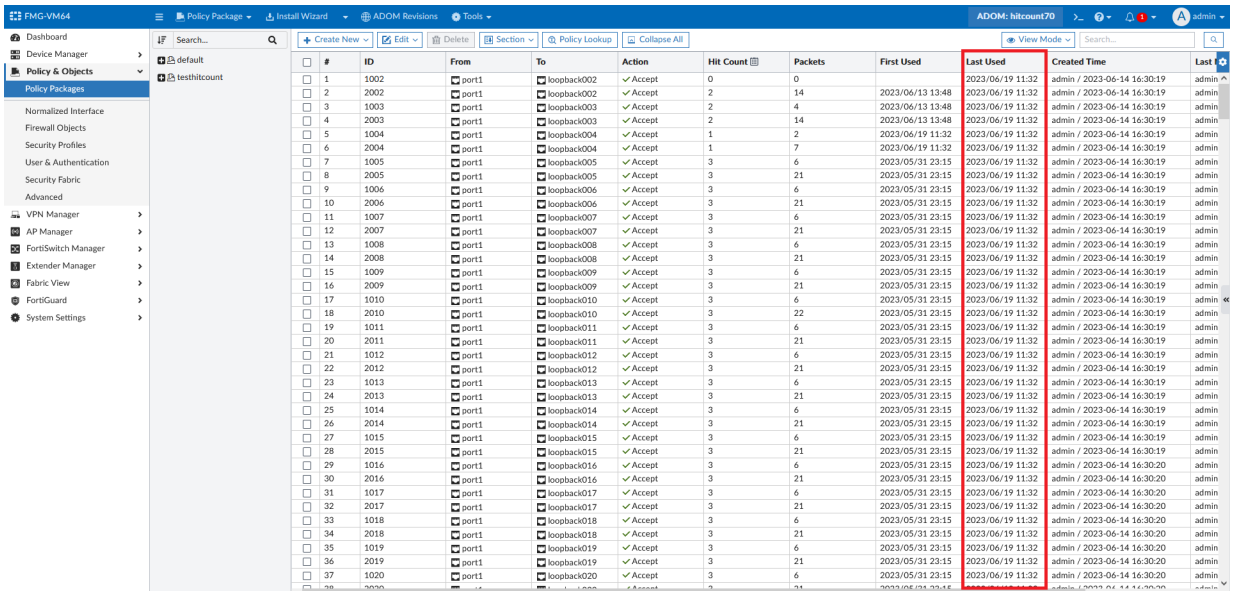
1. In the FortiManager CLI, enter the following command to enable `save-last-hit-in-adomdb`.

   ```
   config system global
   set save-last-hit-in-adomdb enable
   end
   ```

2. Enter the following command to view the "Last Used" timestamp value in the CLI.

   ```
   exe fmpolicy print-adom-package <adom> <packageName> <policy-id>
   ```

3. Go to *Policy & Objects* > *Policy Packages*, and enable the *Last Used* column in *Column Settings*.
4. In the *Tools* dropdown, select *Refresh Hit Counts*.
   In the following example, if the policy id `1002` hit count information (Hit Count/Packets/First Used/Last Used) are reset on the FortiGate side, `1002`'s "Last Used" value (`2023/06/19 11:32`) will *not* be cleared on FortiManager.



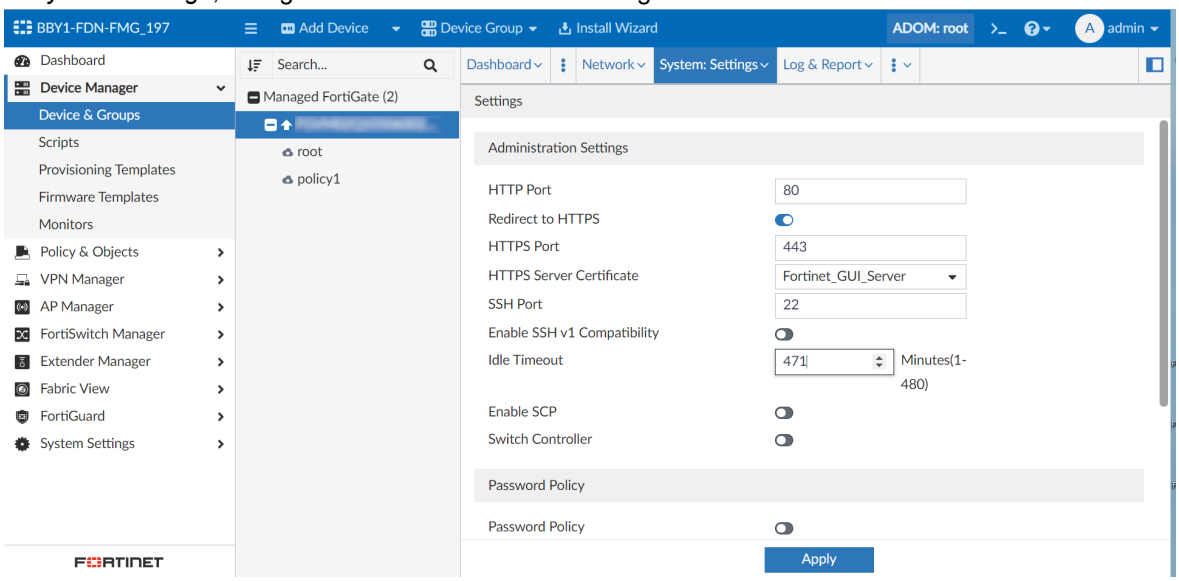
The next time *Refresh Hit Counts* is clicked, if a non-blank value is received as the new "Last Used" timestamp that is more recent than the stored value (`2023/06/19 11:32`), it will be updated and displayed.

Partial install pushes only the instructed configuration (JSON API) - 7.4.1

FortiManager 7.4.1 supports partial installs to push only the instructed configuration (using JSON API) without other pending changes on the device database to better address the role separation between different admin types.

Example of a partial install using JSON API

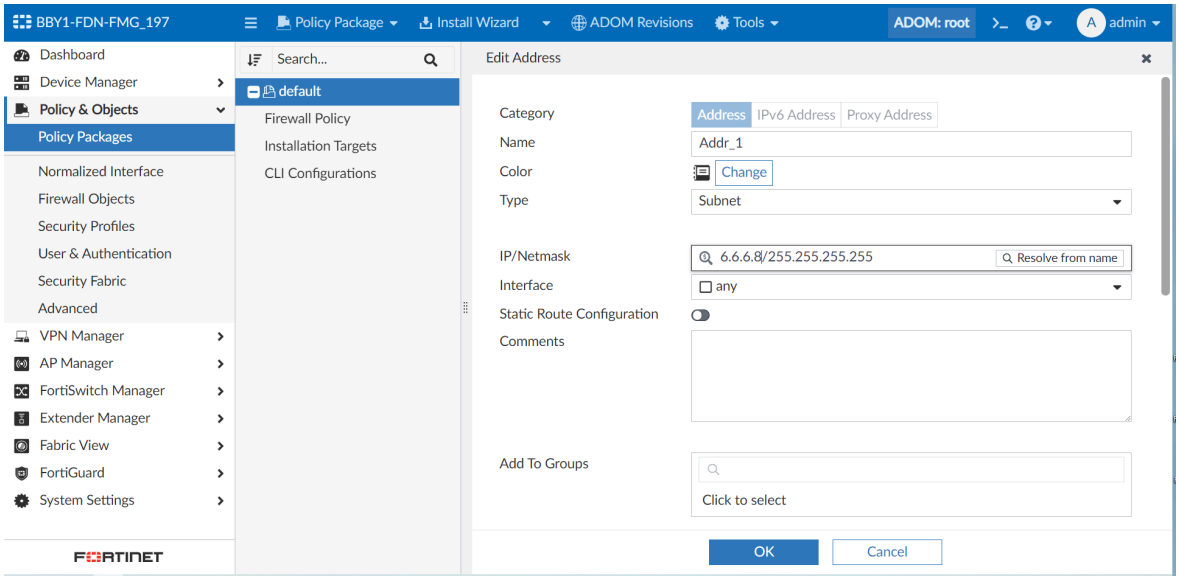
1. Make changes to the managed device. In this example, two changes are made:
   a. Change the device *Idle Timeout* setting:
      i. Go to *Device Manager* > *Device & Groups* and edit a managed device.
      ii. In *System Settings*, change the device *Idle Timeout* setting to 471.



b. Change an address in *Policy & Objects*.

i. Go to *Policy & Objects* > *Policy Packages* and edit a policy package.

ii. Change an address to `6.6.6.8/32`.



2. Using the FortiManager JSON API, perform a partial install. In this example, only the changes to the address are specified.

```
{
"method": "exec",
"params": [
  {
    "data": {
        "adom": "root",
        "objects": [
            ["update", "obj/firewall/address/Addr_1", "", ""]
        ],
        "flags": 0
    },
    "url": "securityconsole/install/objects/v2"
  }
],
"session":
"4Itgh5MwczfkFt9xmpYZcKVhc0iLvcjWV5XPl71yjxwhEDEIkP4HscHfCdk68yx7p7RGILVkCLAY8QHcc3jl+A=
="
}

{

    "result": [

        {

            "data": {

                "task": 22

            },
```

```
            "status": {
                "code": 0,
                "message": "OK"
            },
            "url": "securityconsole/install/objects/v2"
        }
    ]
}
```


3. The install log shows only the address change was installed as intended. The change to the *Idle Timeout* setting was not installed.

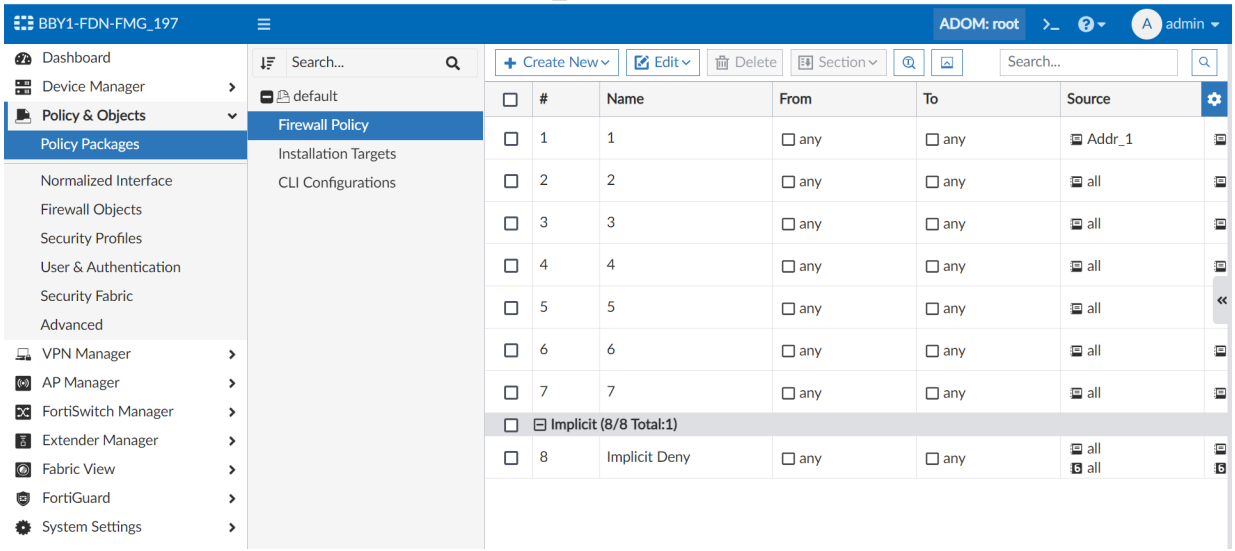
```
Start installing
FortiGate-VM64 $  config vdom
FortiGate-VM64 (vdom) $  edit root
current vf=root:0
FortiGate-VM64 (root) $  config firewall address
FortiGate-VM64 (address) $  edit "Addr_1"
FortiGate-VM64 (Addr_1) $  set subnet 6.6.6.8 255.255.255.255
FortiGate-VM64 (Addr_1) $  next
FortiGate-VM64 (address) $  end
FortiGate-VM64 (root) $  end
---> generating verification report
<--- done generating verification report
install finished
```

Policy partial install supports policy reorder/move operation (JSON API) - 7.4.1

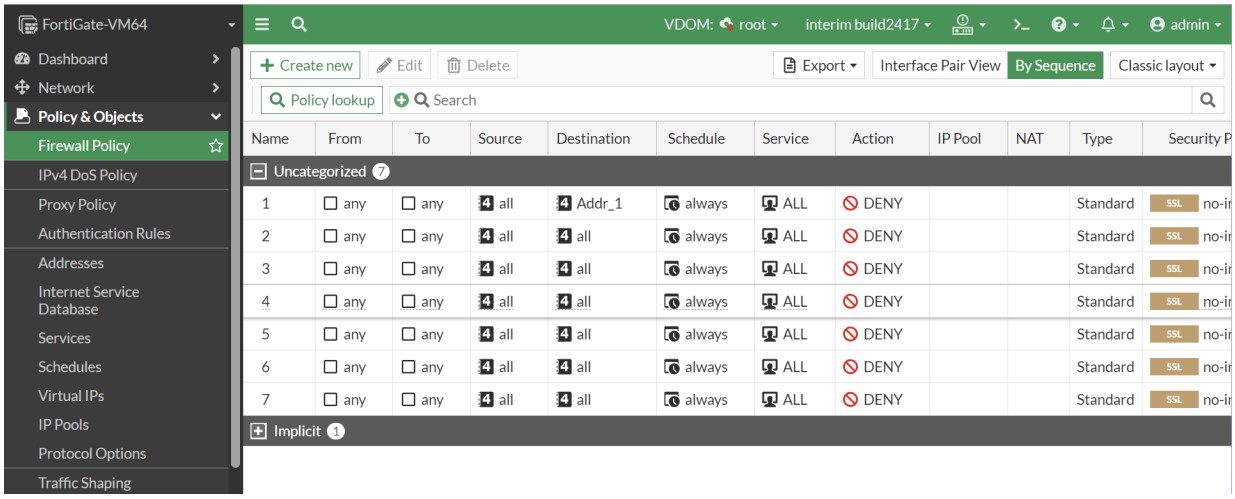
Policy partial install (JSON API) supports policy reorder/move operation.

Example of a reorder/move operation in partial installs using JSON API

1. In this example, seven policies and address `Addr_1` are created in a Policy Package.

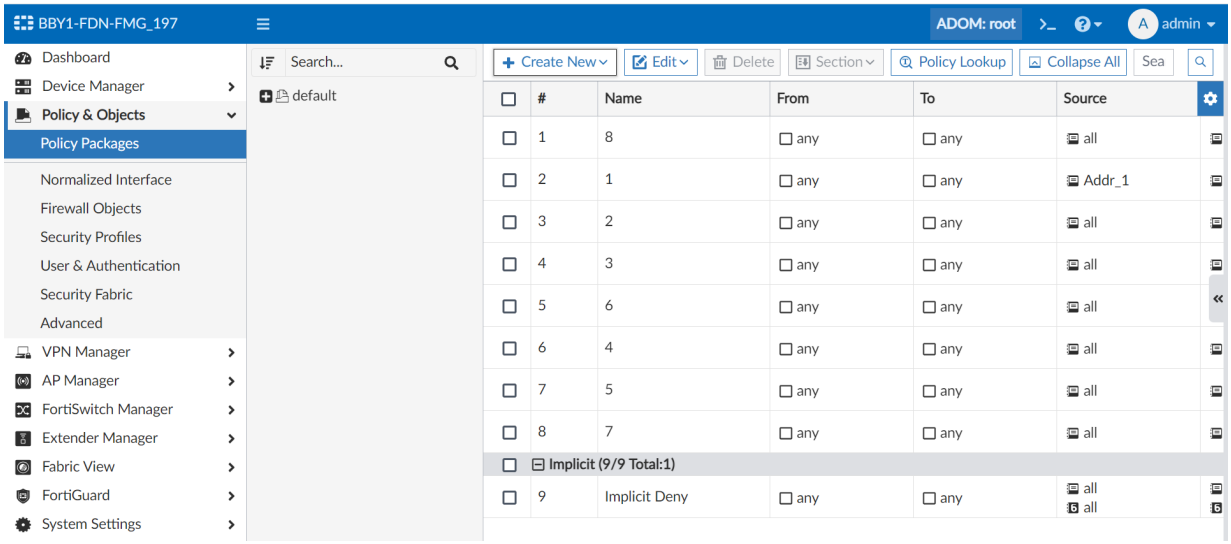


2. Install the policies to a FortiGate.



3. Perform the following modifications on the Policy Package.
   a. Create one new policy and move it before policy 1.
   b. Change Addr_1 IP.
   c. Move policy 6 after policy 3.

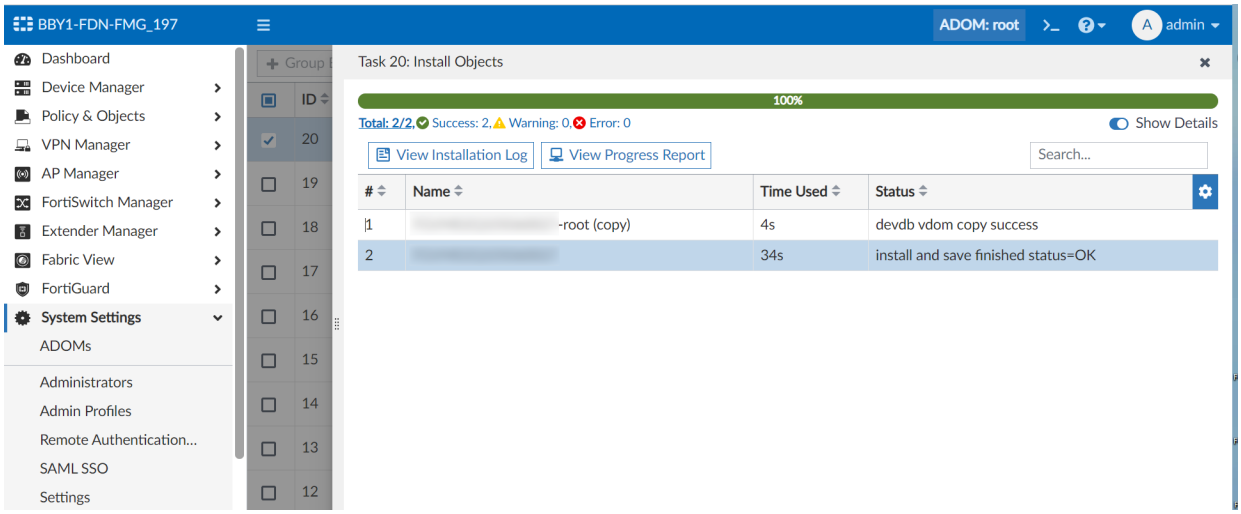
d. Delete policy 4.



4. Using JSON API, perform a partial install.

```
Post:

{
"method": "exec",
"params": [
  {
    "data": {
        "adom": "root",
        "objects": [
            ["add", "pkg/default/firewall/policy/9", "before", "1"],
            ["update", "obj/firewall/address/Addr_1", "", ""],
            ["delete", "pkg/default/firewall/policy/4", "", ""],
            ["move", "pkg/default/firewall/policy/6", "after", "3"]
        ],
        "flags": 0
    },
    "url": "securityconsole/install/objects/v2"
  }
],
"session":
"msWfmFWGIJyDX/LRYaOPFALvGjgjJ82yzV2s919g1DWgVY1r1HFJu1o4+xsOQCSdA0kyiSwB5DrXsl2rW0vEmw=
="
}

Response:
{
    "result": [
        {
            "data": {
                "task": 20
            },
            "status": {
                "code": 0,
                "message": "OK"
            },
```

```
            "url": "securityconsole/install/objects/v2"
        }
    ]
}
```

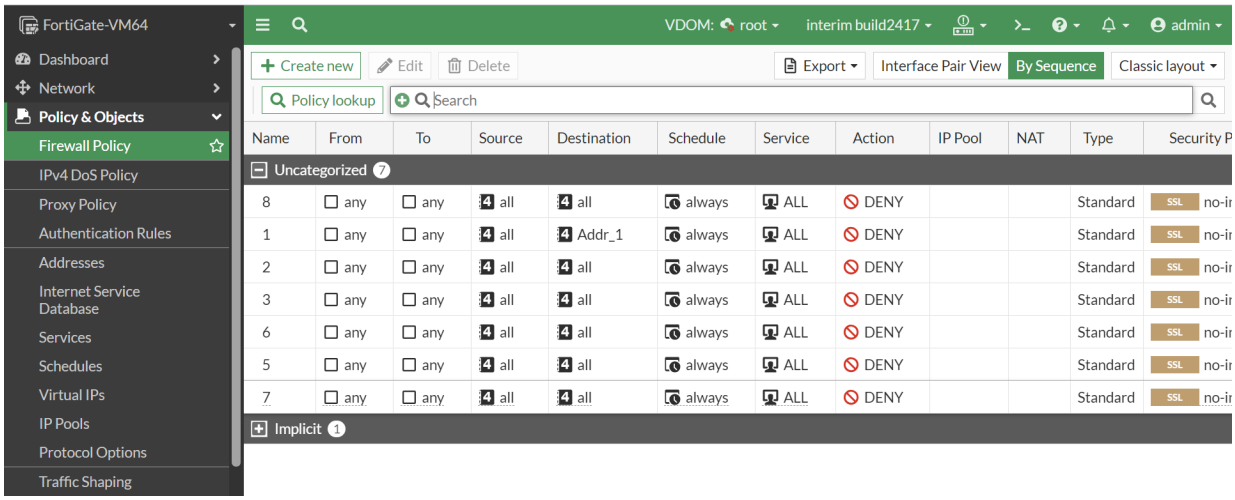


5. View the install log.

```
View Install Log

Starting log (Run on device)

Start installing

FortiGate-VM64 $  config vdom

FortiGate-VM64 (vdom) $  edit root

current vf=root:0

FortiGate-VM64 (root) $  config firewall policy

FortiGate-VM64 (policy) $  delete 4

FortiGate-VM64 (policy) $  end

FortiGate-VM64 (root) $  config firewall address

FortiGate-VM64 (address) $  edit "Addr_1"

FortiGate-VM64 (Addr_1) $  set subnet 6.6.6.7 255.255.255.255

FortiGate-VM64 (Addr_1) $  next

FortiGate-VM64 (address) $  end

FortiGate-VM64 (root) $  config firewall policy

FortiGate-VM64 (policy) $  edit 9

FortiGate-VM64 (9) $  set name "8"

FortiGate-VM64 (9) $  set uuid 798858d0-2506-51ee-2c43-da0bf419ad7d

FortiGate-VM64 (9) $  set srcintf "any"

FortiGate-VM64 (9) $  set dstintf "any"

FortiGate-VM64 (9) $  set srcaddr "all"
```

```
FortiGate-VM64 (9) $  set dstaddr "all"
FortiGate-VM64 (9) $  set schedule "always"
FortiGate-VM64 (9) $  set service "ALL"
FortiGate-VM64 (9) $  set logtraffic all
FortiGate-VM64 (9) $  next
FortiGate-VM64 (policy) $  move 9 before 1
FortiGate-VM64 (policy) $  move 5 after 6
FortiGate-VM64 (policy) $  end
FortiGate-VM64 (root) $  end
---> generating verification report
<--- done generating verification report
install finished
```

6. All changes are installed to the FortiGate.



System

This section lists the new features added to FortiManager for system settings:

High Availability (HA)

This section lists the new features added to FortiManager for high availability (HA):

FortiManager supports different VM type platforms to form the FortiManager cluster

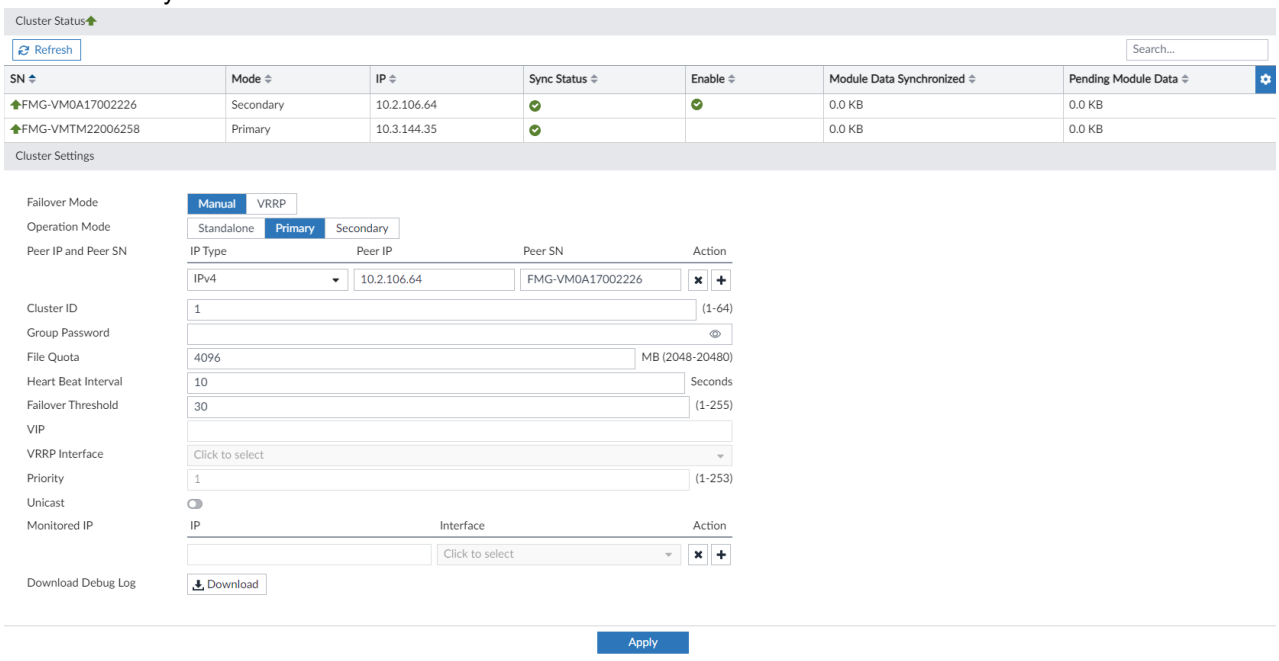
This information is also available in the FortiManager 7.4 Administration Guide:

- High Availability

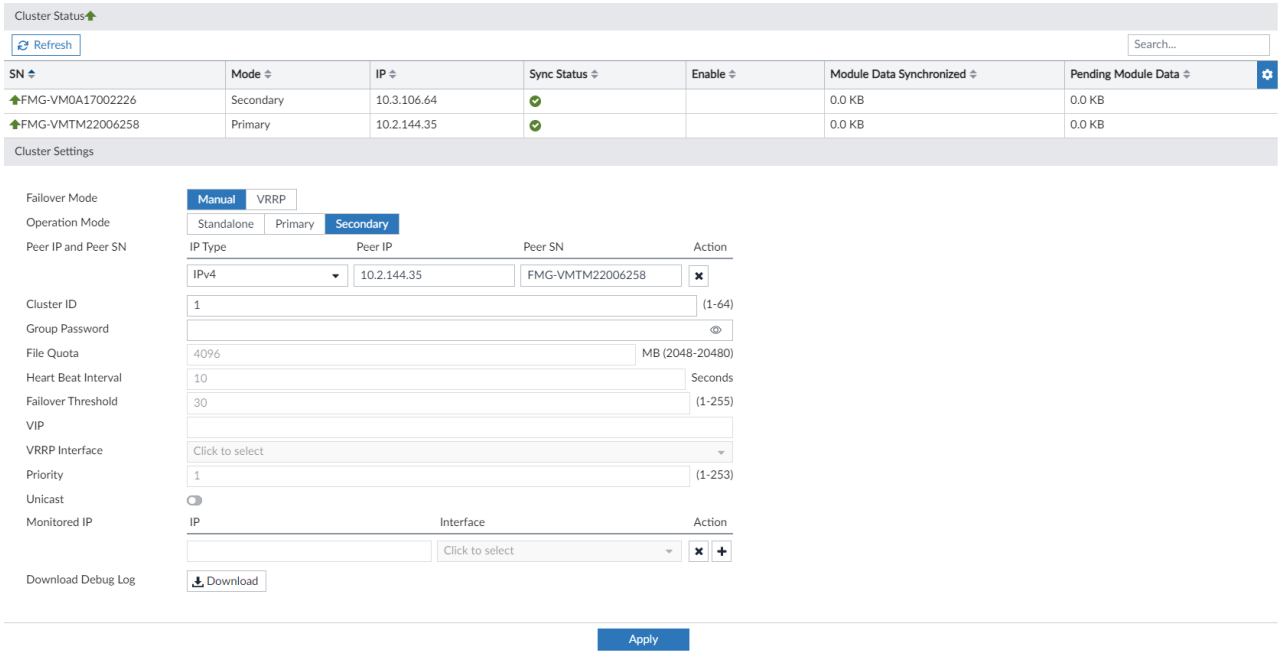
FortiManager supports different VM type platforms to form the FortiManager cluster.

Below is an example of a FortiManager HA formed with FMG-VM64-KVM as the Primary device and FMG-VM64 as the secondary. The steps to configure HA have not changed.

- For the Primary HA device:



- For the Secondary HA device:



ADOM

This section lists the new features added to FortiManager for ADOMs:

- ADOM 7.2 Policy Package supports installation on FortiGate 7.4 7.4.1 on page 93
- 7.2 ADOM managing mixed FOS versions 7.4.1 on page 96
- FortiManager can upgrade multiple ADOMs (same version) at the same time 7.4.1 on page 98

ADOM 7.2 Policy Package supports installation on FortiGate 7.4 - 7.4.1

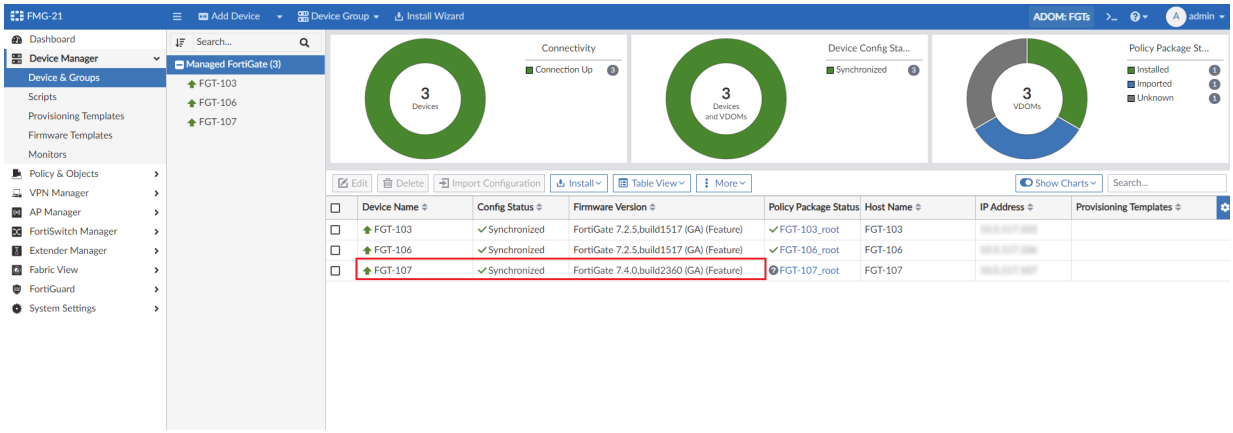
This information is also available in the FortiManager 7.4 Administration Guide:

- Using Mixed Versions in ADOMs

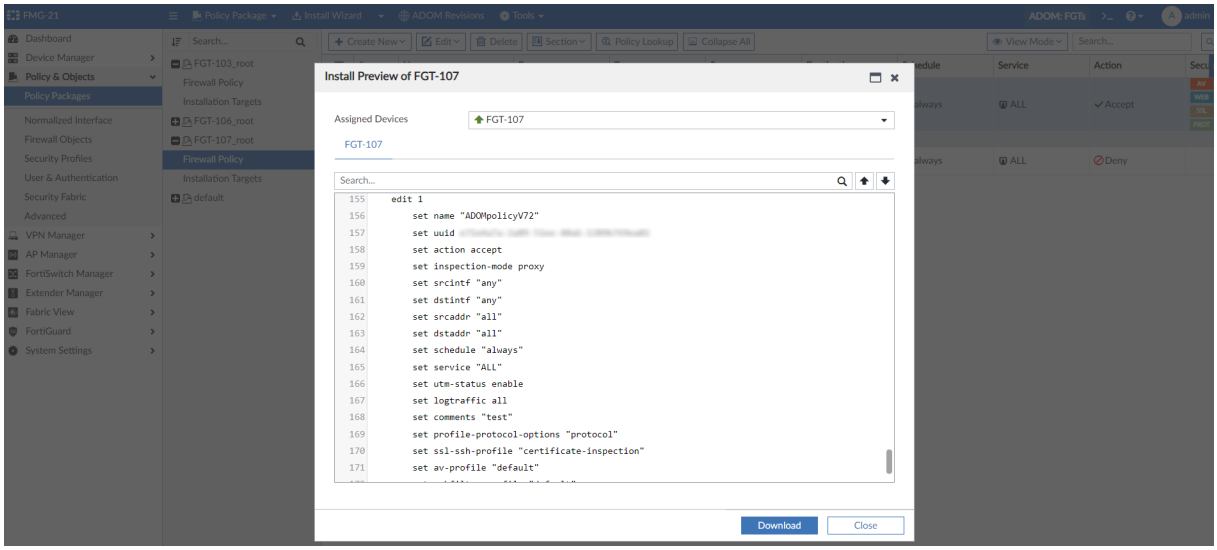
FortiManager ADOM 7.2 Policy Packages support installation on FortiGates on version 7.4.

- ADOMs on version 7.2 are normally used to manage FortiGate devices on version 7.2 but in some cases you may need to upgrade some managed FortiGate units in the ADOM from 7.2 to 7.4. FortiManager can install 7.2 policy

packages to FortiGate 7.4 devices.

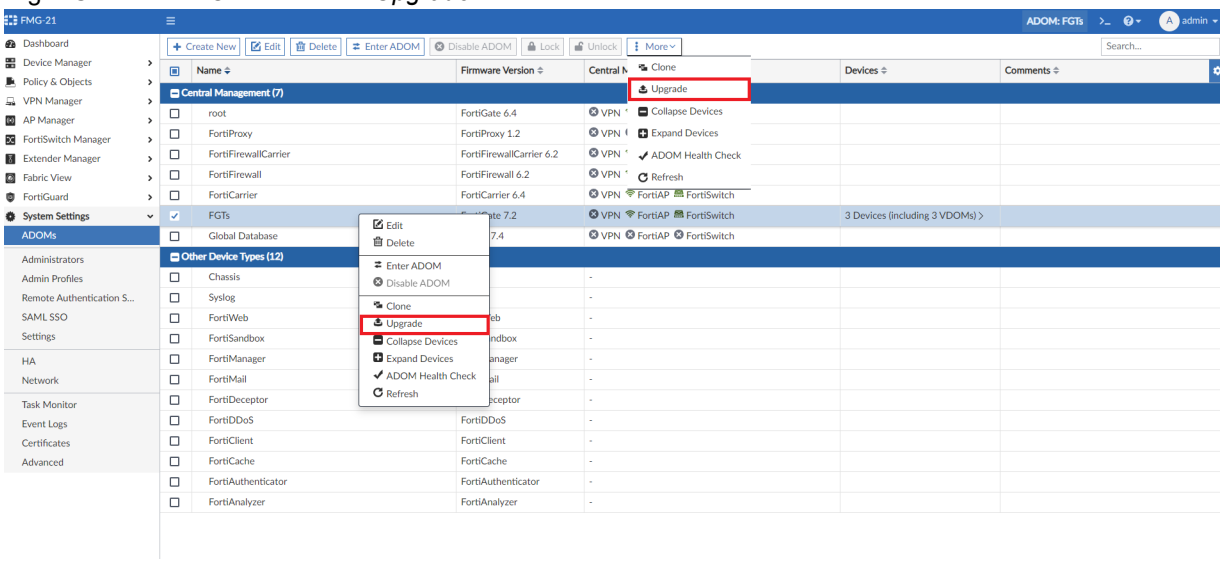


- When you create a firewall policy in a 7.2 ADOM and install it to a FortiGate 7.4 device, FortiManager's backend system automatically handles the 7.4 syntax. FortiManager doesn't change any new 7.4 features on the FortiGate 7.4 unit.

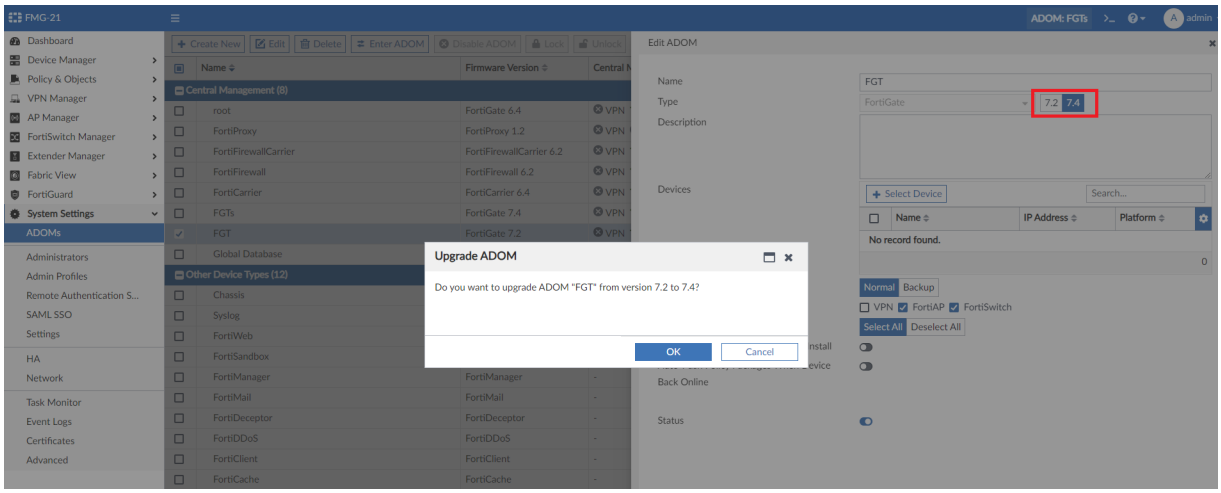


There are three ways to upgrade an ADOM from version 7.2 to 7.4:

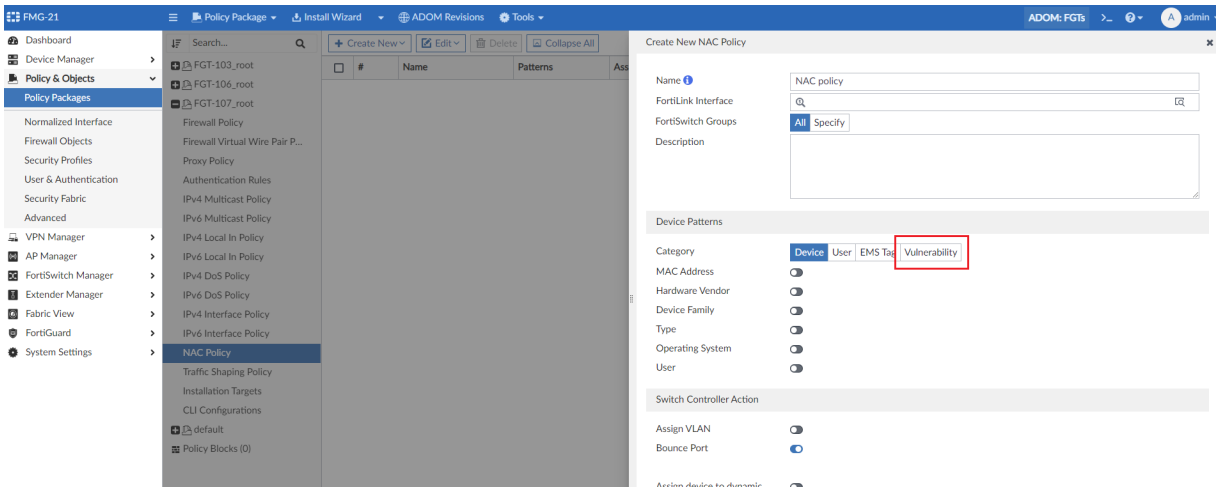
1. Navigate to *System Settings* > *ADOMs* > *More* > *Upgrade*.
2. Right-Click the ADOM and select *Upgrade*.



3. Edit the ADOM to select to the next version 7.4.



After upgrading the ADOM from 7.2 to 7.4, all of the database objects are automatically converted to the 7.4 format and the GUI reflects new 7.4 features.



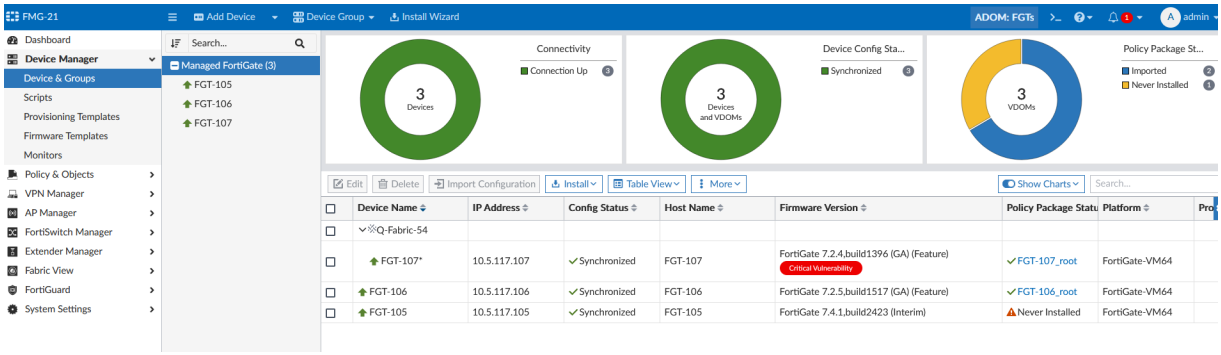
7.2 ADOM managing mixed FOS versions - 7.4.1

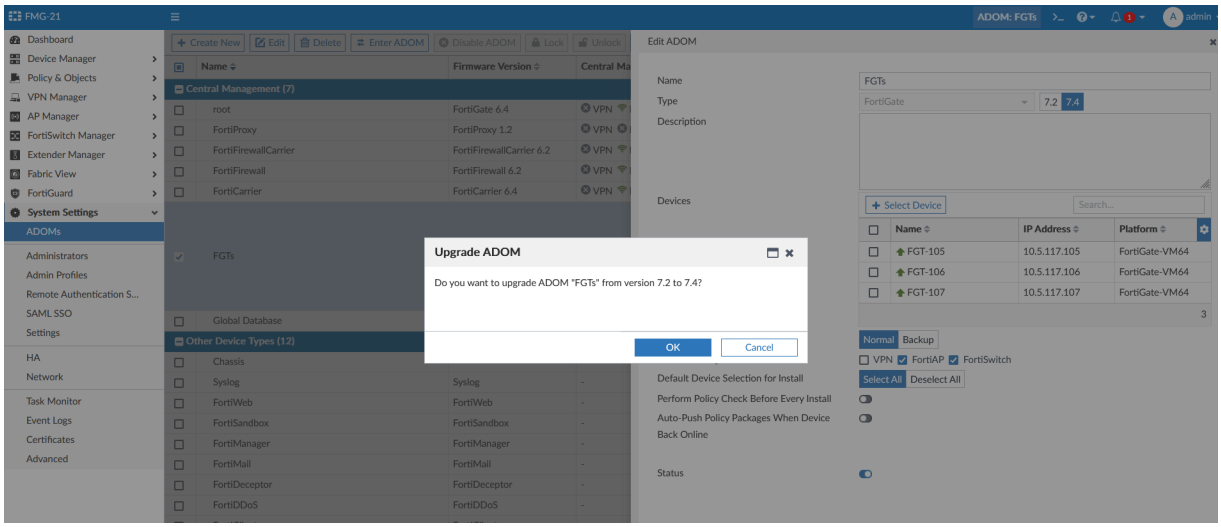
This information is also available in the FortiManager 7.4 Administration Guide:

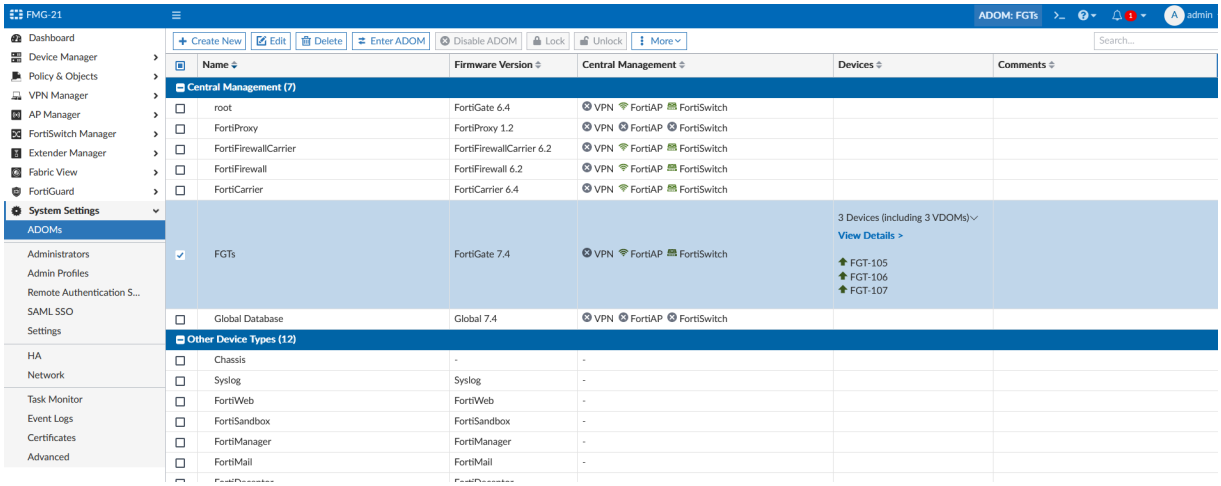
- Using Mixed Versions in ADOMs

When a 7.2 ADOM is managing mixed FOS versions (FortiOS 7.2 and 7.4), the ADOM can be upgraded to version 7.4.

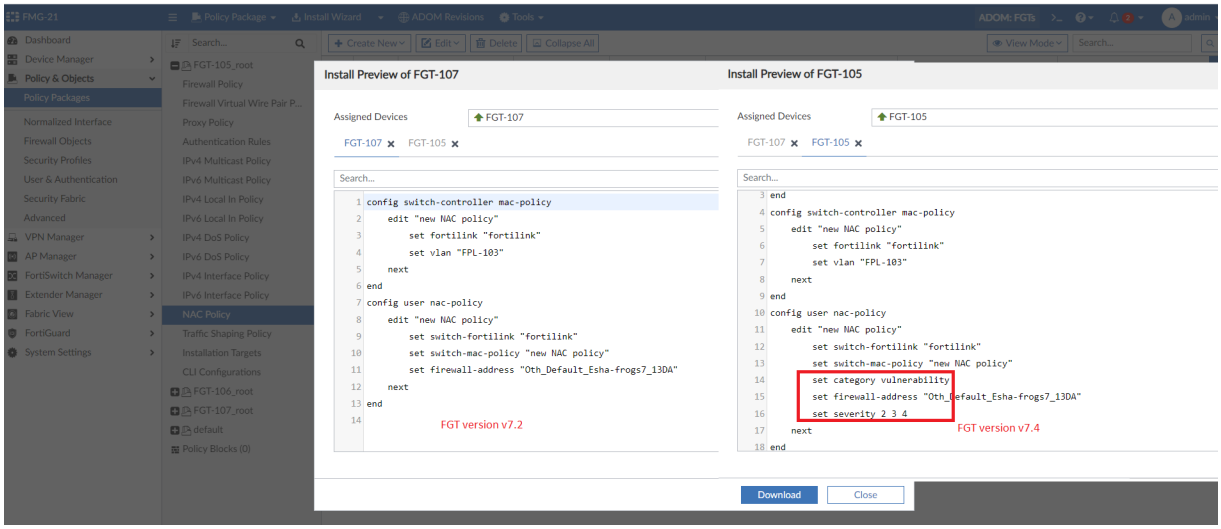
- When FortiManager is managing mixed FortiGate units running on FortiOS 7.2 and FortiOS 7.4 in an 7.2 ADOM, FortiManager allows you to upgrade the ADOM from 7.2 to 7.4 before upgrading all FortiGates in the ADOM to FortiOS 7.4.



- 

- 

- In the upgraded 7.4 ADOM, you can create new 7.4 firewall policies and install the policy to both FortiGate devices on FortiOS 7.4 and 7.2. FortiManager's backend system automatically downgrades the 7.4 syntax to the 7.2 version when installed to a FortiOS 7.2 device.



FortiManager can upgrade multiple ADOMs (same version) at the same time - 7.4.1

This information is also available in the FortiManager 7.4 Administration Guide:

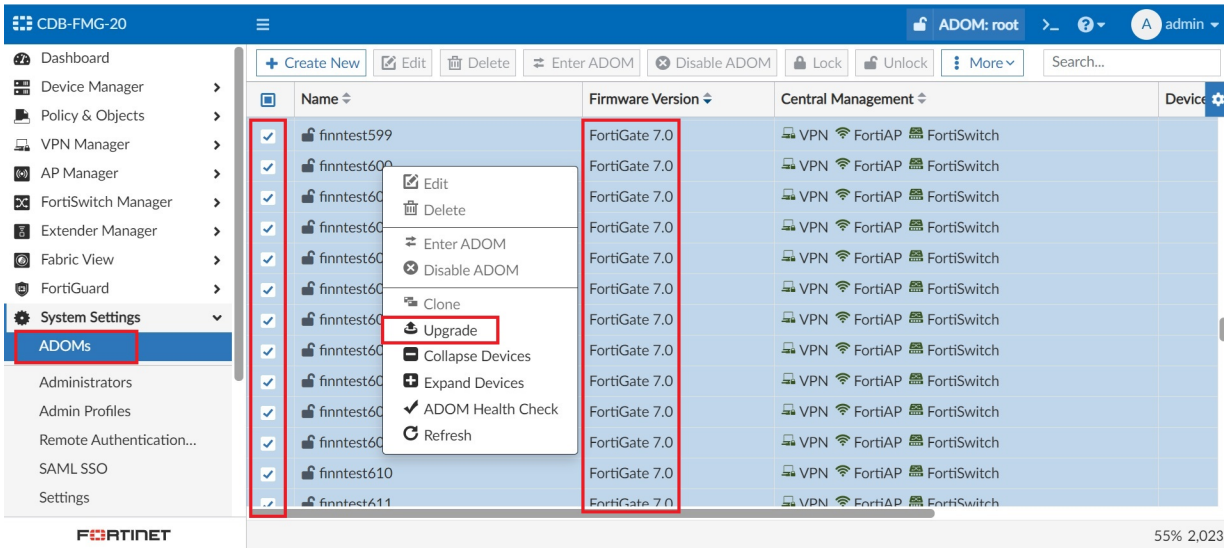
- Upgrading an ADOM

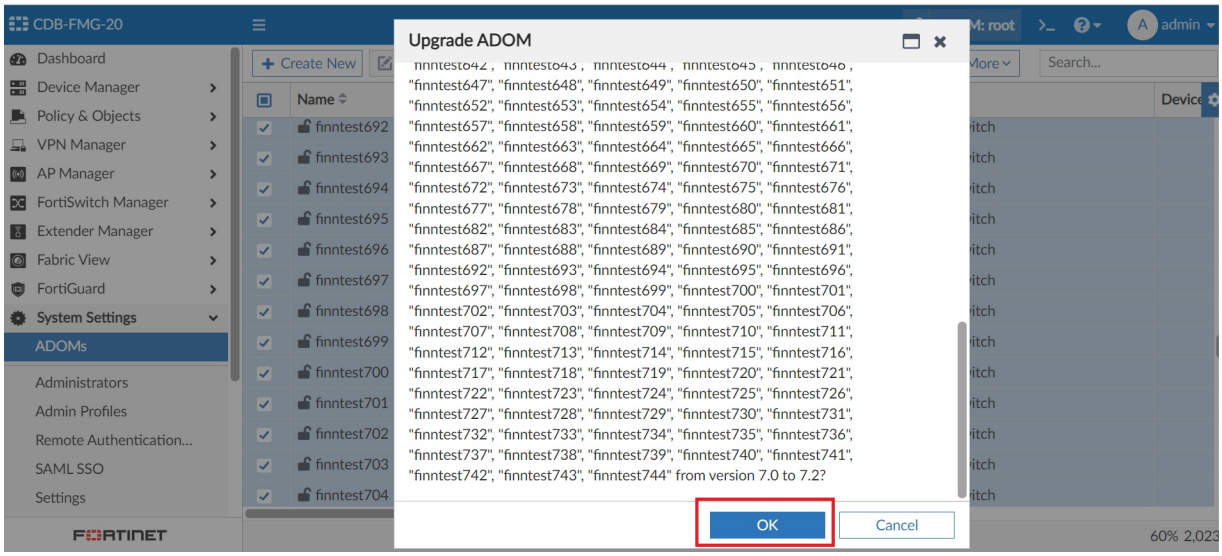
FortiManager is able to upgrade multiple ADOMs on the same version at the same time.

To upgrade multiple ADOMs at the same time:

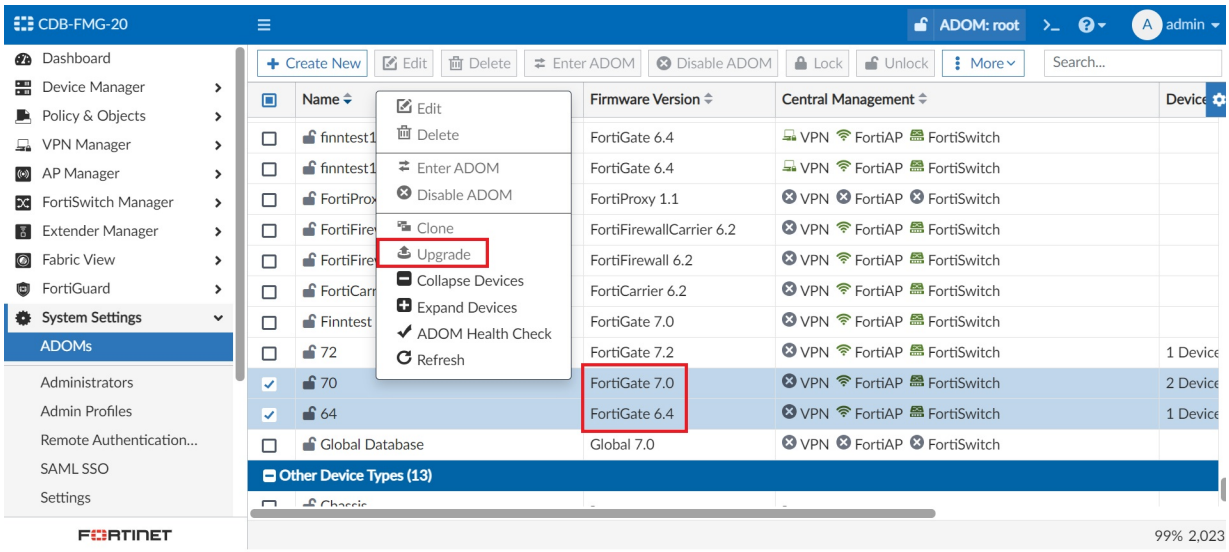
1. Go to *System Settings* > *ADOMs*.
2. Select multiple ADOMs of the same version in the ADOM table and do one of the following:
   a. Right-click on a selected device in the table and select *Upgrade*.
   b. Select *More* > *Upgrade* in the toolbar.

   In this example, the customer has 200 ADOMs and they want to upgrade their ADOMs at the same time. Each ADOM is on version 7.0 and has one managed FortiGate device. FortiManager can upgrade all of the ADOMs at the same time.





In this example, the customer has one ADOM on 7.0 and another on 6.4. When both ADOMs are selected, the upgrade button is unavailable because the ADOMs are on different versions. The ADOMs cannot be upgraded at the same time.



Others

This section lists the new features added to FortiManager for other features relating to system settings:

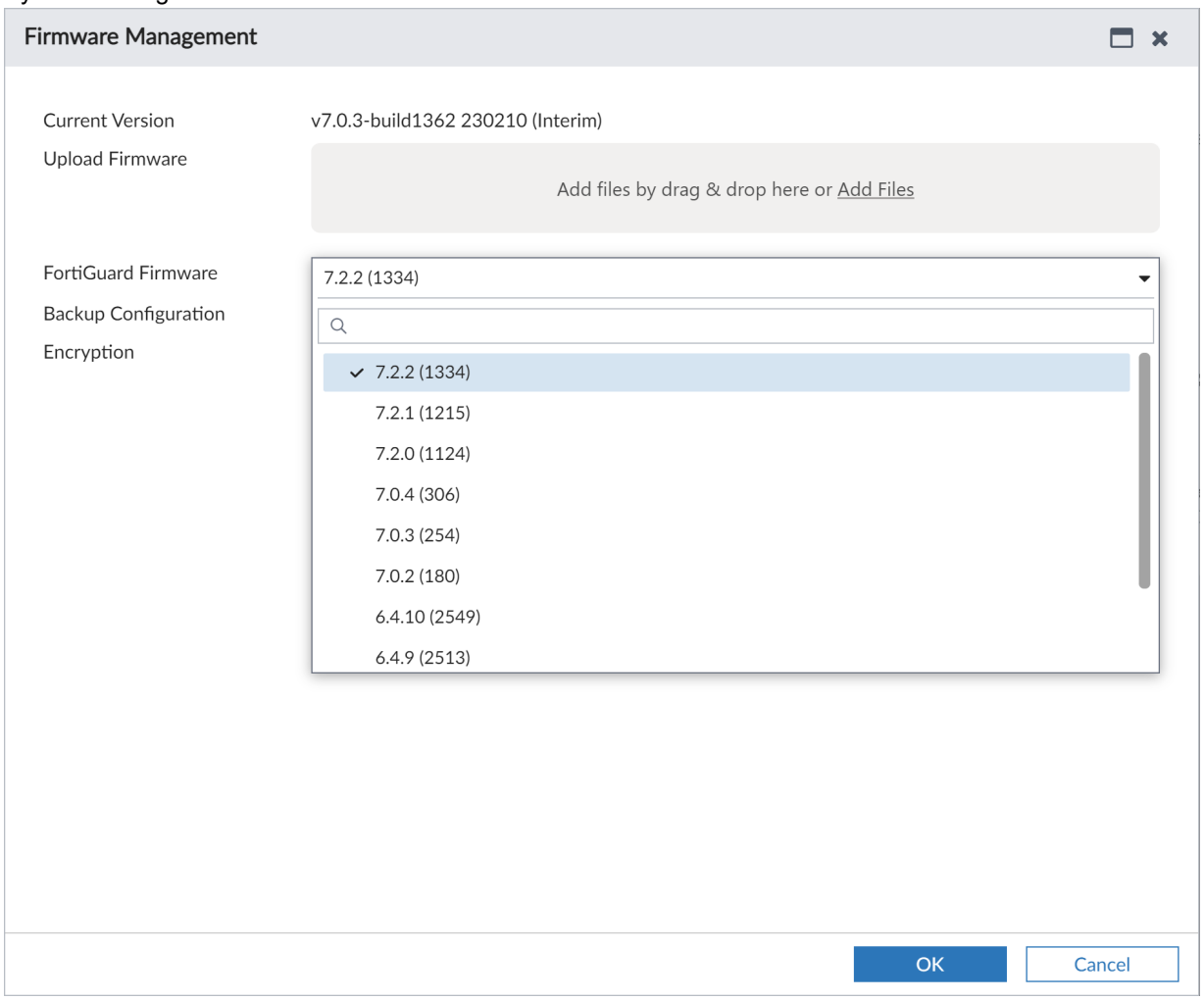
- Block out contract device from upgrading to next or major or minor release on page 100
- Automatic system backup setup in GUI to configure a backup schedule and visualize backup history 7.4.1 on page 102

Block out contract device from upgrading to next or major or minor release

This information is also available in the FortiManager 7.4 Administration Guide:
- Updating the system firmware.

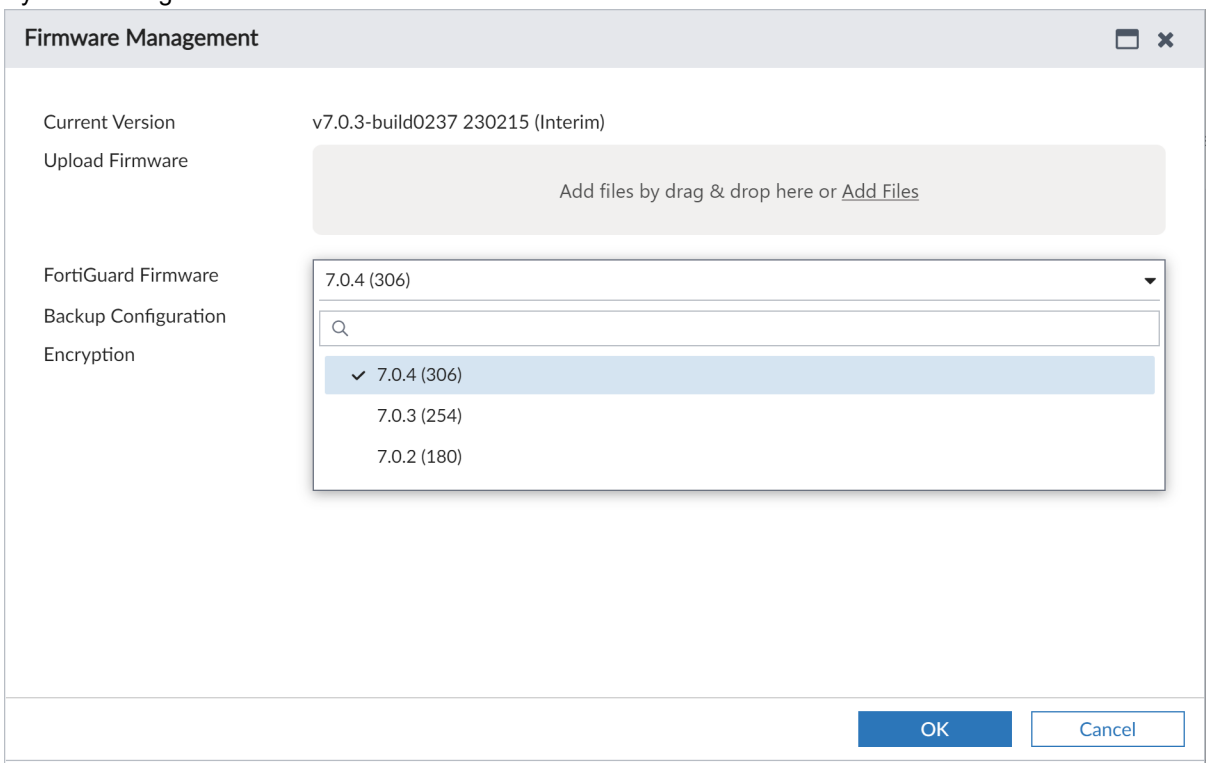
To view available FortiGuard images:

1. A FortiManager with a valid contract will display all available FortiGuard images and allow upgrading or downgrading to any version.
   - System Settings:

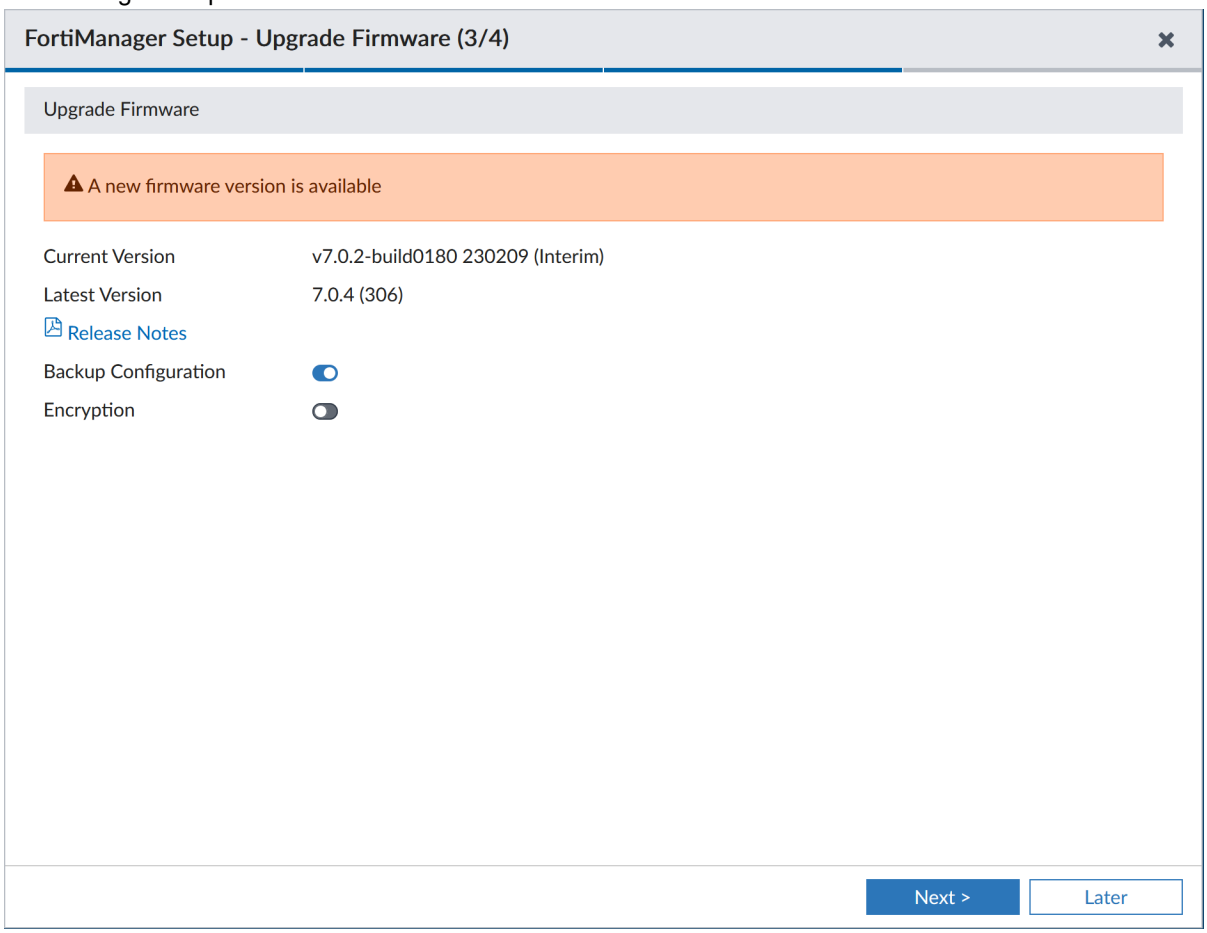


2. A FortiManager without a valid contract or with an expired contract will only display available patch images and support patch upgrades.

- System Settings:



- FortiManager setup wizard:



Automatic system backup setup in GUI to configure a backup schedule and visualize backup history - 7.4.1

This information is also available in the FortiManager 7.4 Administration Guide:

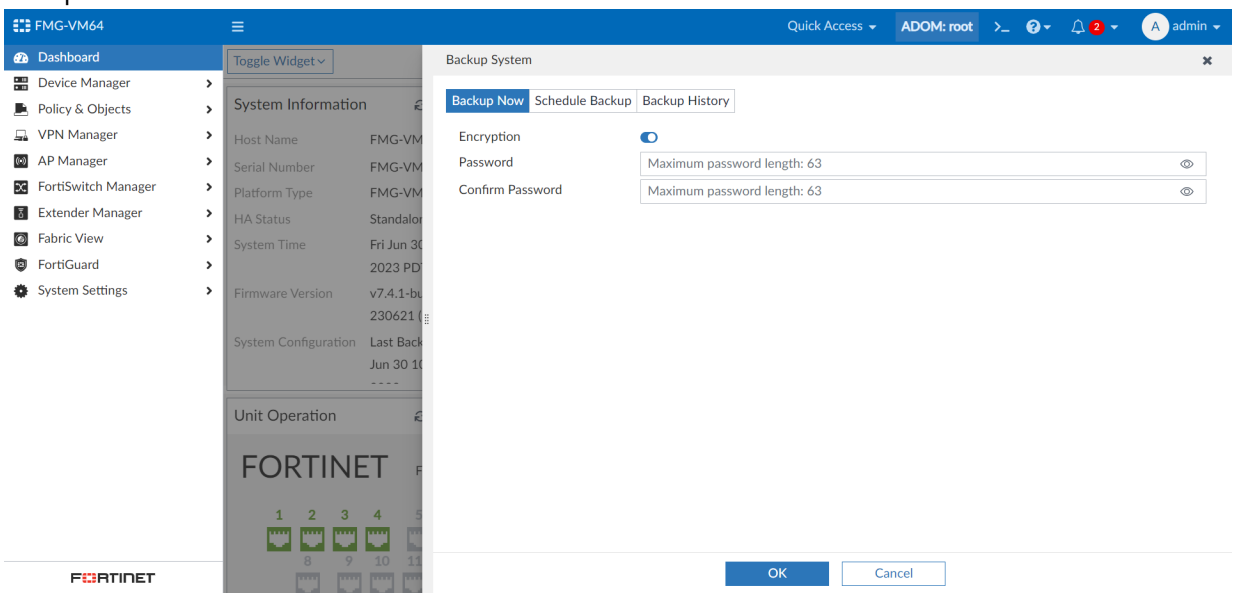
- Backing up the system

Automatic system backup setup is available in the FortiManager GUI to configure a backup schedule and visualize the backup history.

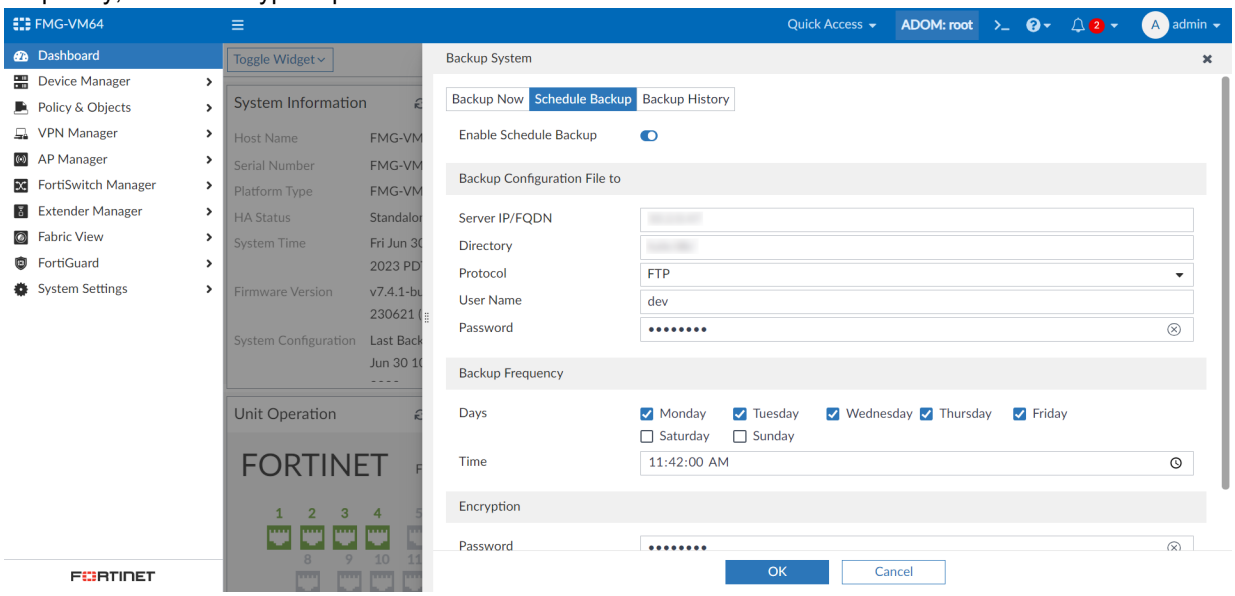
To configure scheduled backups and view backup history in the GUI:

1. Go to *Dashboard*.

2. In the *System Information* widget, click the backup button next to *System Configuration*. The *Backup System* dialog box opens.

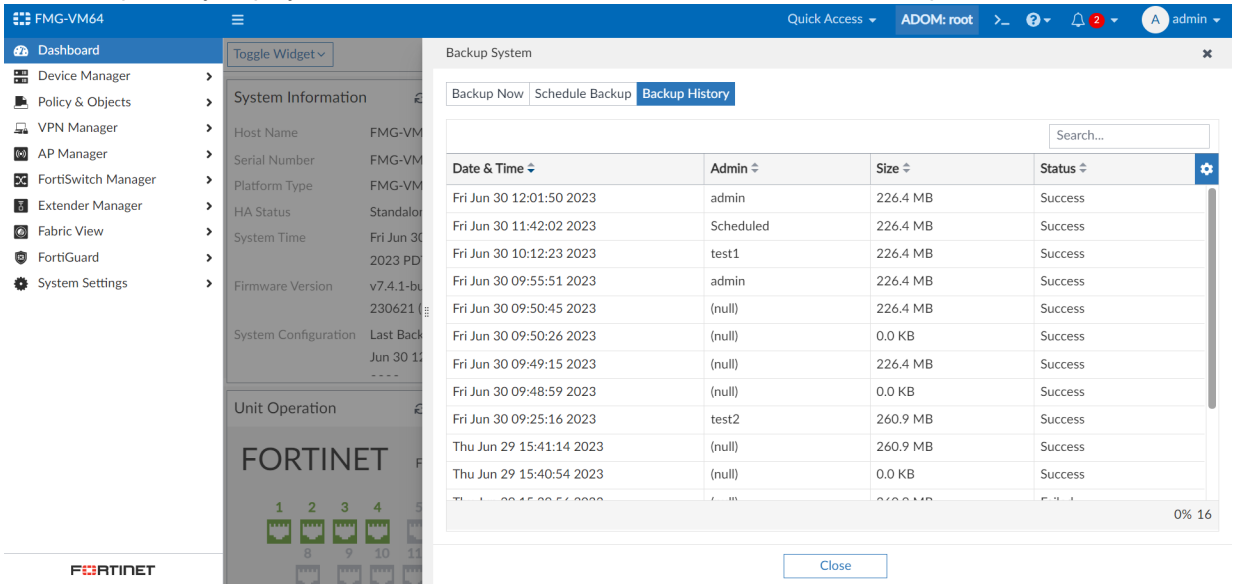


3. Select the *Schedule Backup* tab.
4. Enable the *Enable Schedule Backup* option, and configure the options including the backup location, backup frequency, and an encryption password.



5. Click *OK*.

6. Select the *Backup History* tab.
   The backup history displays the *Date & Time*, *Admin*, *Size* and *Status* of each backup.



Cloud Services

This section lists the new features added to FortiManager for cloud services:

FortiManager used as single-pane management tool to orchestrate FortiGate deployment in AWS

FortiManager used as single-pane management tool to orchestrate FortiGate deployment in AWS.

This information is also available in the FortiManager 7.4 Administration Guide:

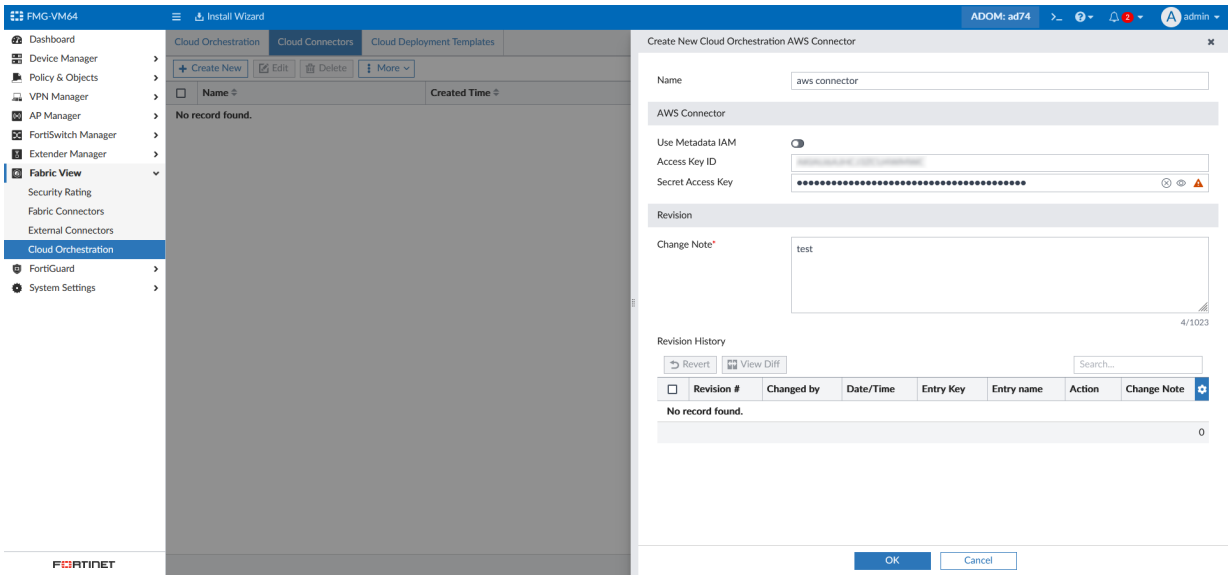
- Cloud Orchestration

FortiManager *Fabric View* adds Cloud Orchestration with the following panes:

- Cloud Orchestration
- Cloud Connectors
- Cloud Deployment Templates

To configure cloud orchestration using FortiManager:

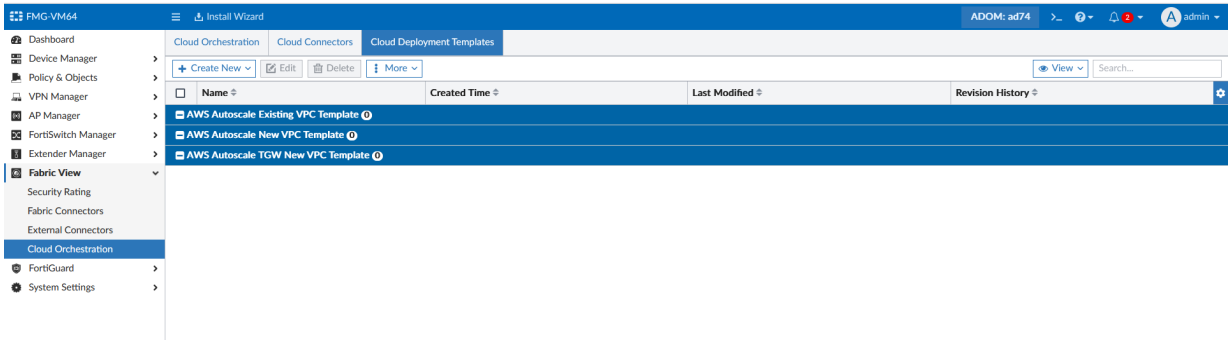
1. Create an AWS cloud orchestration connector:
   a. Go to *Fabric View* > *Cloud Orchestration* > *Cloud Connectors*.
   b. Click *Create New*.
   c. Configure the AWS connector to connect to your AWS server.
   You can enable *Use Metadata IAM* for FortiManager AWS instances using IAM.



d. Click *OK*.

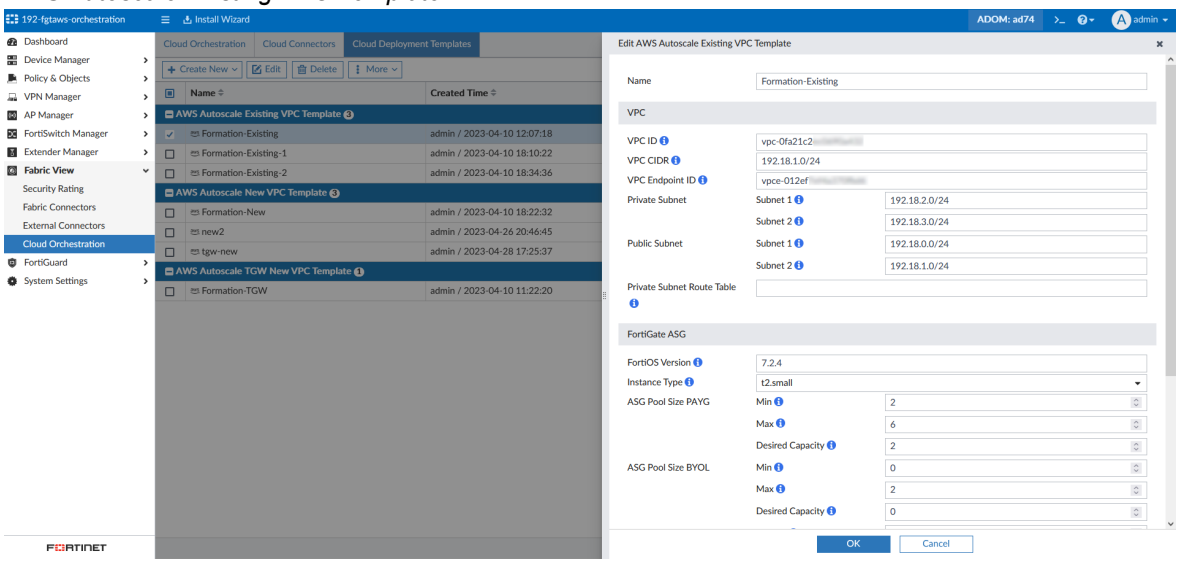
2. Create a cloud deployment template:

a. Go to *Fabric View* > *Cloud Orchestration* > *Cloud Deployment Templates*.

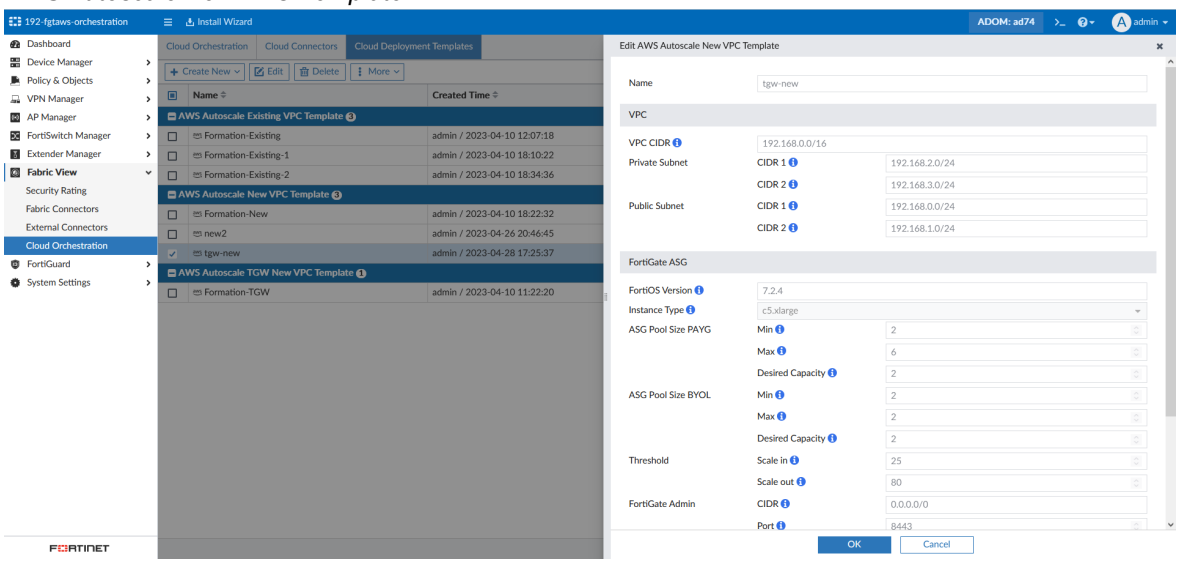


b. Click Create New, and select a deployment template type. There are three template types available:

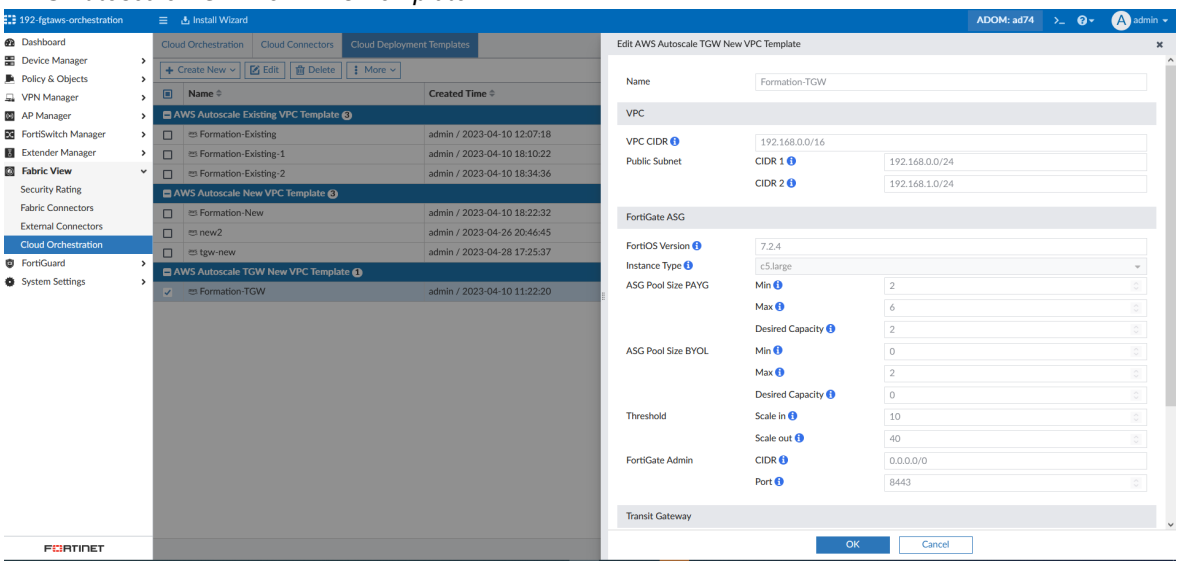
i. *AWS Autoscale Existing VPC Template*



ii. *AWS Autoscale New VPC Template*



iii. *AWS Autoscale TGW New VPC Template*



c. Configure the details for your chosen template, including the virtual private cloud (VPC) and FortiGate autoscale group (ASG) settings.

d. Click *OK*.

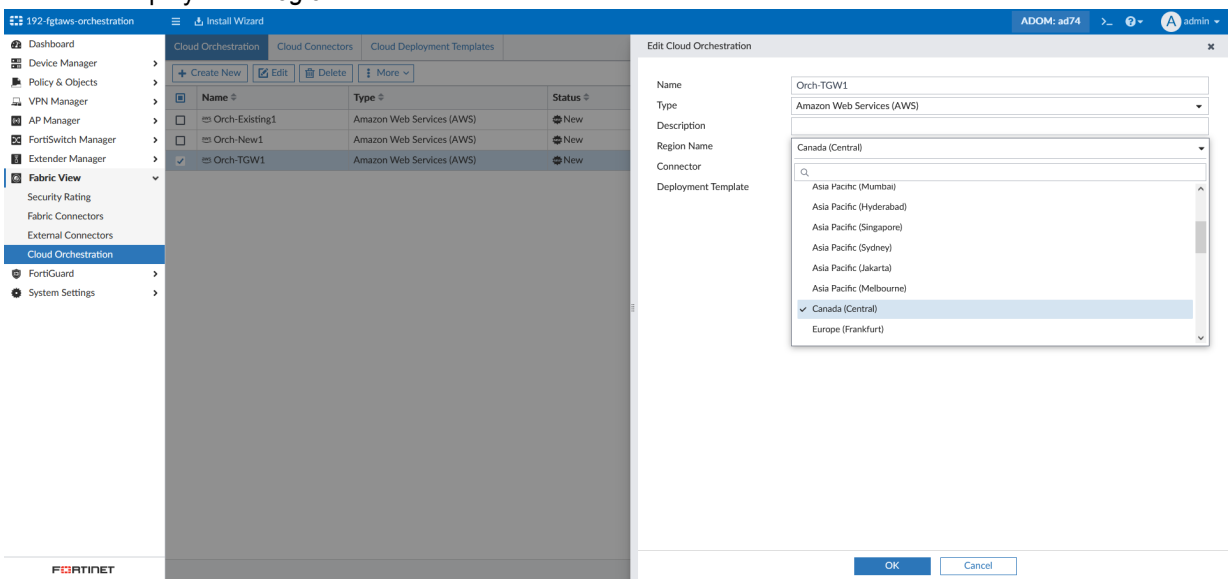
3. Configure cloud orchestration:

a. Go to *Fabric View* > *Cloud Orchestration* > *Cloud Orchestration*.

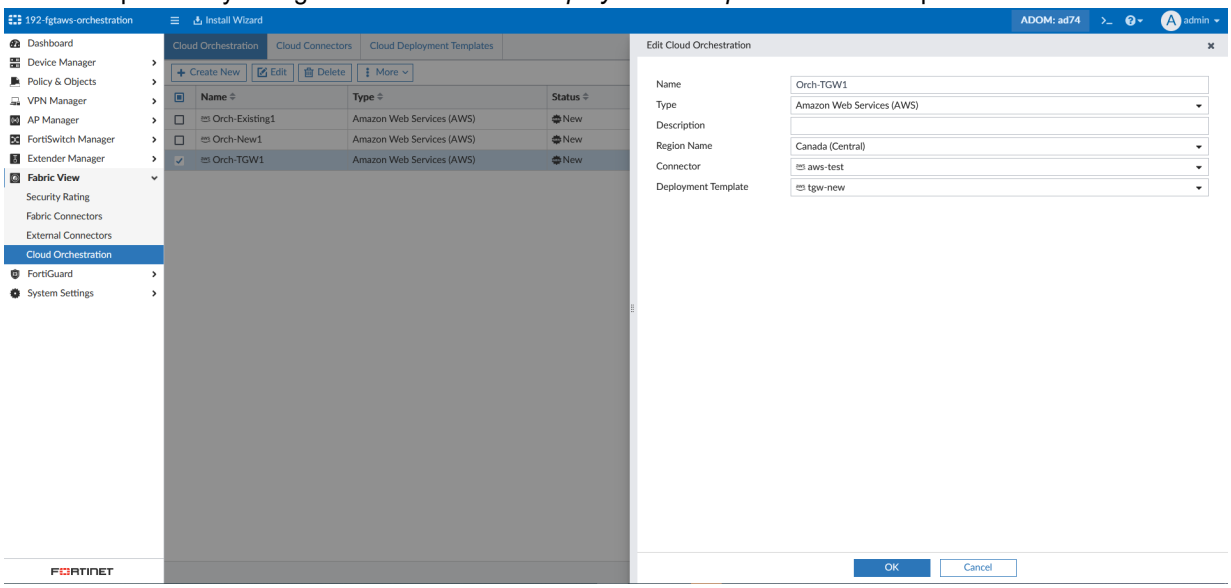
b. Click *Create New*.

c. Enter a *Name* and optional *Description* for your cloud orchestration.

d. Select the deployment *Region*.



e. Select the previously configured *Connector* and *Deployment Template* from the dropdown menus.

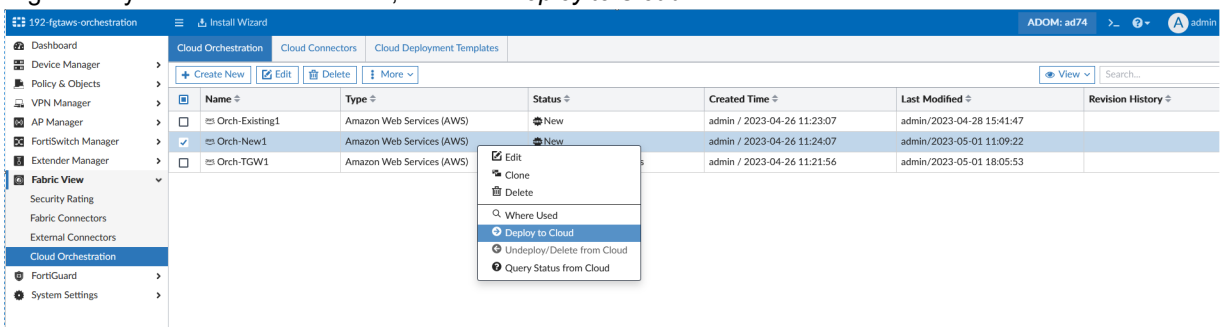


f. Click *OK*.

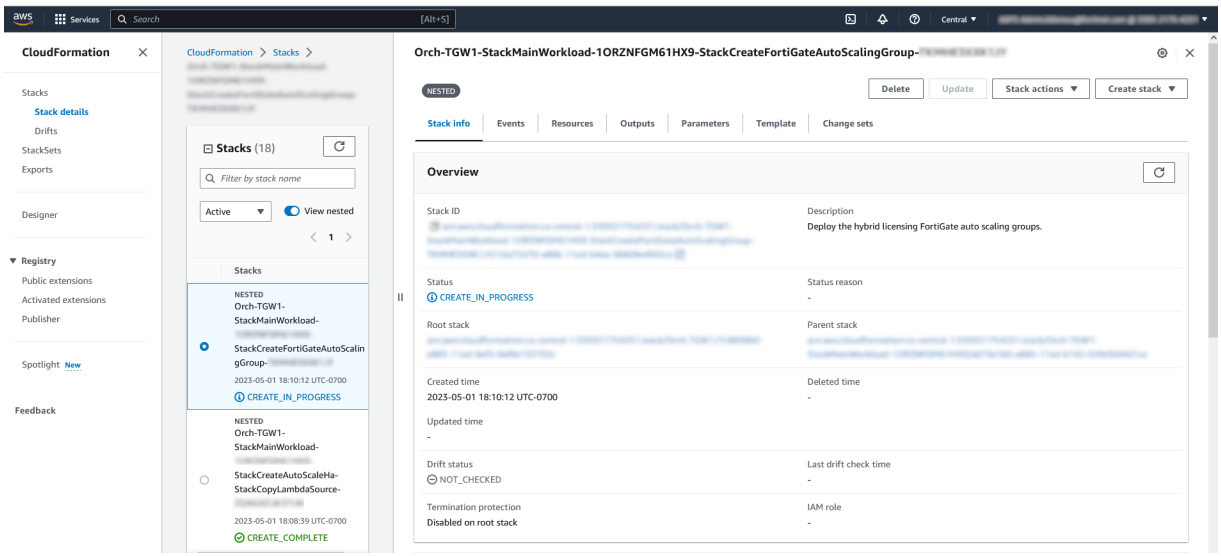
4. Deploy to cloud:

a. Go to *Fabric View* > *Cloud Orchestration* > *Cloud Orchestration*.

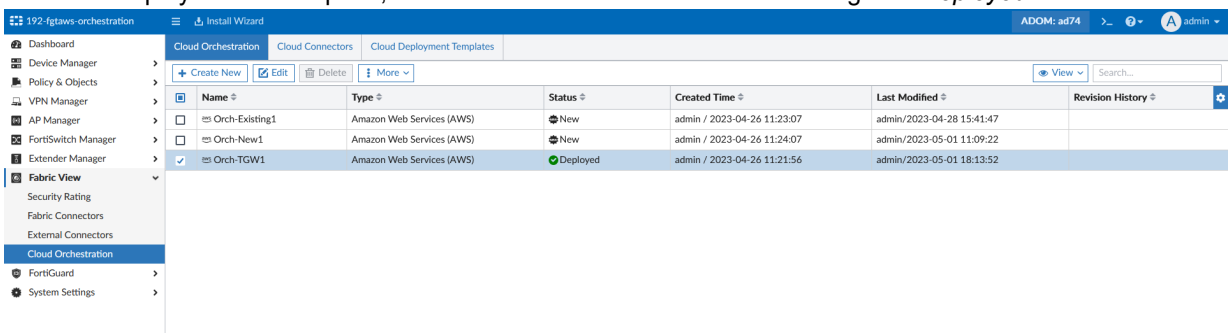
b. Right click your cloud orchestration, and click *Deploy to Cloud*.



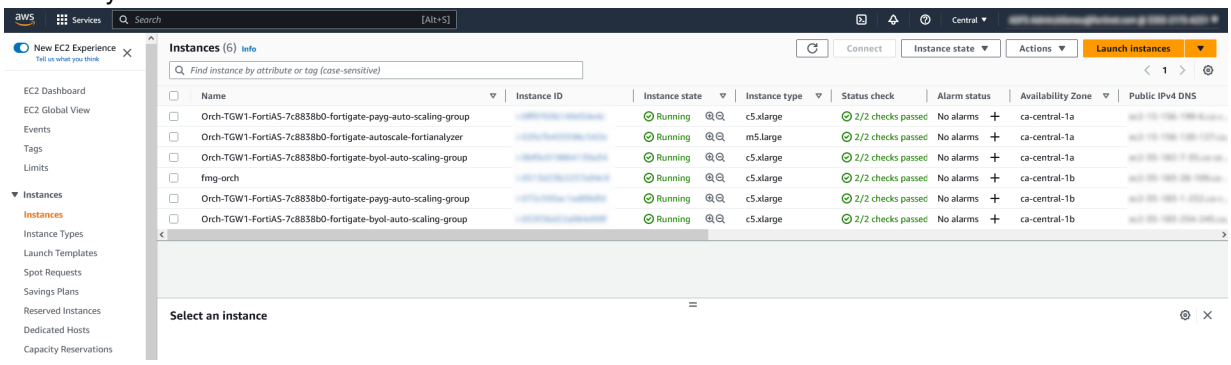
AWS CloudFormation shows the deploy as *CREATE_IN_PROGRESS*.



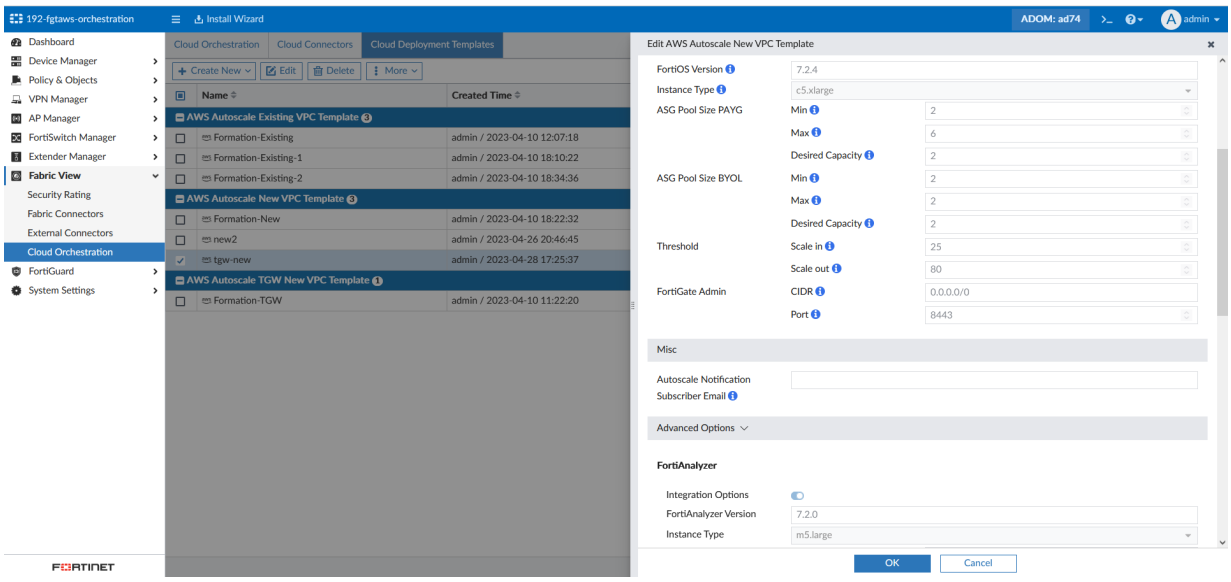
When the deployment is complete, the status of the cloud orchestration changes to *Deployed*.



Check on AWS EC2 to confirm the instances are deployed as expected.
In this example the cloud orchestration has deployed 2 FortiGate BYOL, 2 FortiGate PAYG, and 1 FortiAnalyzer.



Compare the settings with the FortiManager Cloud Deployment template to confirm the settings match.


192-fgtaws-orchestration
Install Wizard
ADOM: ad74
admin
Dashboard
Device Manager
Policy & Objects
VPN Manager
AP Manager
FortiSwitch Manager
Extender Manager
Fabric View
Security Rating
Fabric Connectors
External Connectors
Cloud Orchestration
FortiGuard
System Settings
Cloud Orchestration
Cloud Connectors
Cloud Deployment Templates
Create New
Edit
Delete
More
Name
Created Time
AWS Autoscale Existing VPC Template 3
Formation-Existing
admin / 2023-04-10 12:07:18
Formation-Existing-1
admin / 2023-04-10 18:10:22
Formation-Existing-2
admin / 2023-04-10 18:34:36
AWS Autoscale New VPC Template 3
Formation-New
admin / 2023-04-10 18:22:32
new2
admin / 2023-04-26 20:46:45
tgw-new
admin / 2023-04-28 17:25:37
AWS Autoscale TGW New VPC Template 1
Formation-TGW
admin / 2023-04-10 11:22:20
Edit AWS Autoscale New VPC Template
FortiOS Version
7.2.4
Instance Type
c5.xlarge
ASG Pool Size PAYG
Min
2
Max
6
Desired Capacity
2
ASG Pool Size BYOL
Min
2
Max
2
Desired Capacity
2
Threshold
Scale in
25
Scale out
80
FortiGate Admin
CIDR
0.0.0.0/0
Port
8443
Misc
Autoscale Notification
Subscriber Email
Advanced Options
FortiAnalyzer
Integration Options
FortiAnalyzer Version
7.2.0
Instance Type
m5.large
OK
Cancel

Other

This section lists other new features added to FortiManager:

New FortiManager UX design

This information is also available in the FortiManager7.4 Administration Guide:
- GUI Overview

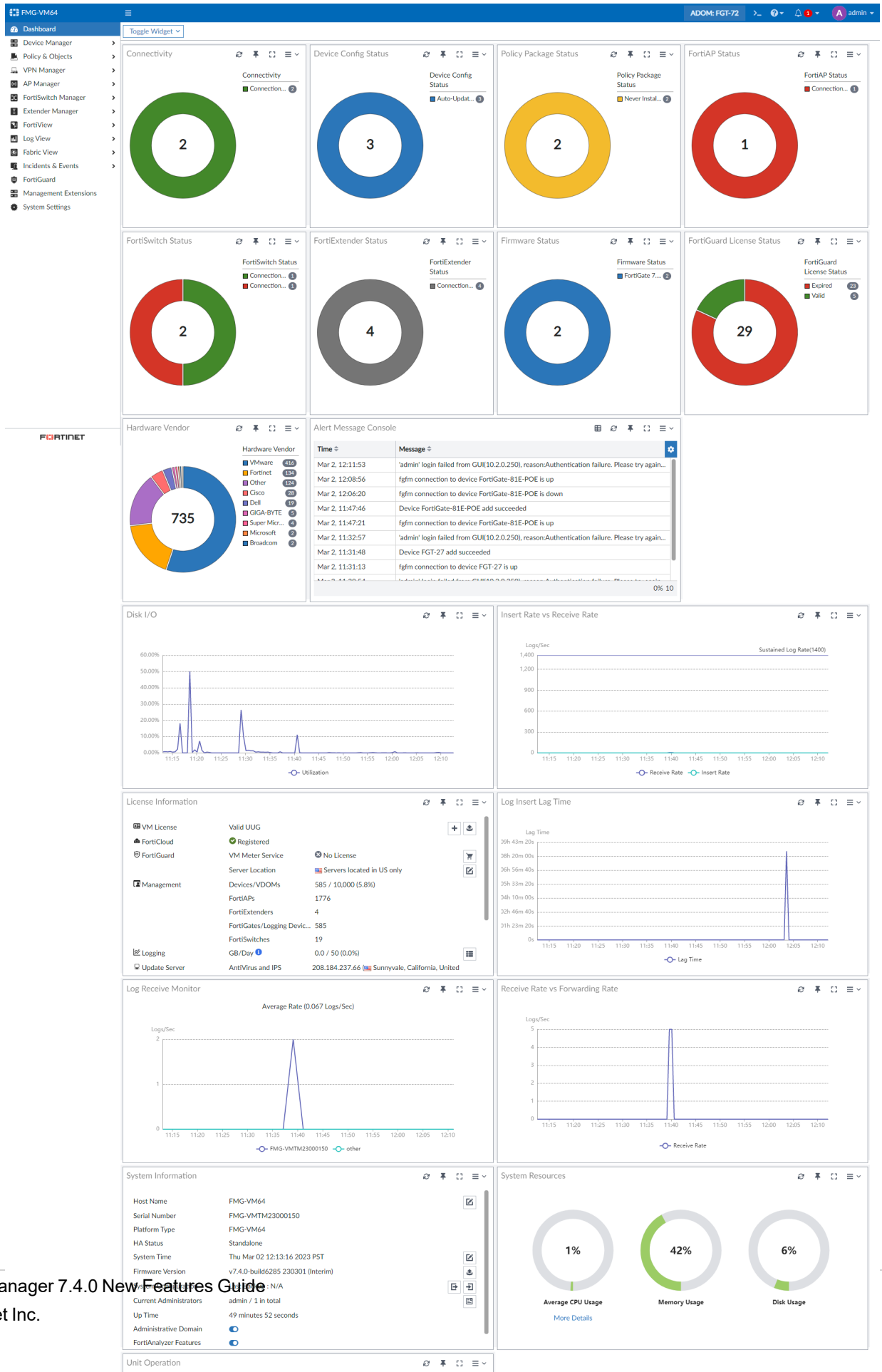
In FortiManager 7.4.0, there is a new FortiManager user experience design that allows for per-admin customizable dashboards and adds a 3-layer left navigation menu to increase accessibility.

The FortiManager GUI now uses a new landing page called *Dashboard*. By default, the dashboard is displayed. You can access other pages, such as *Device Manager*, from the left-pane navigation.

The following new feature topic includes examples of some of the changes to the GUI introduced in FortiManager 7.4.0.

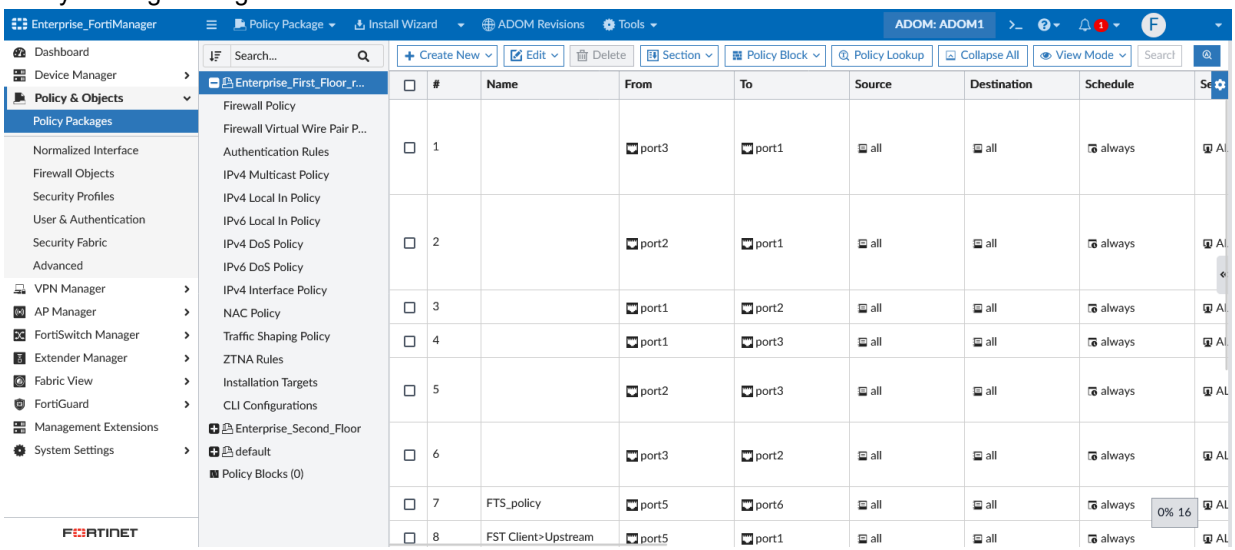
Dashboard

- The *Dashboard* includes widgets, such as *Policy Package Status* and *Firmware Status*. You can toggle which widgets display from the *Toggle Widget* dropdown.

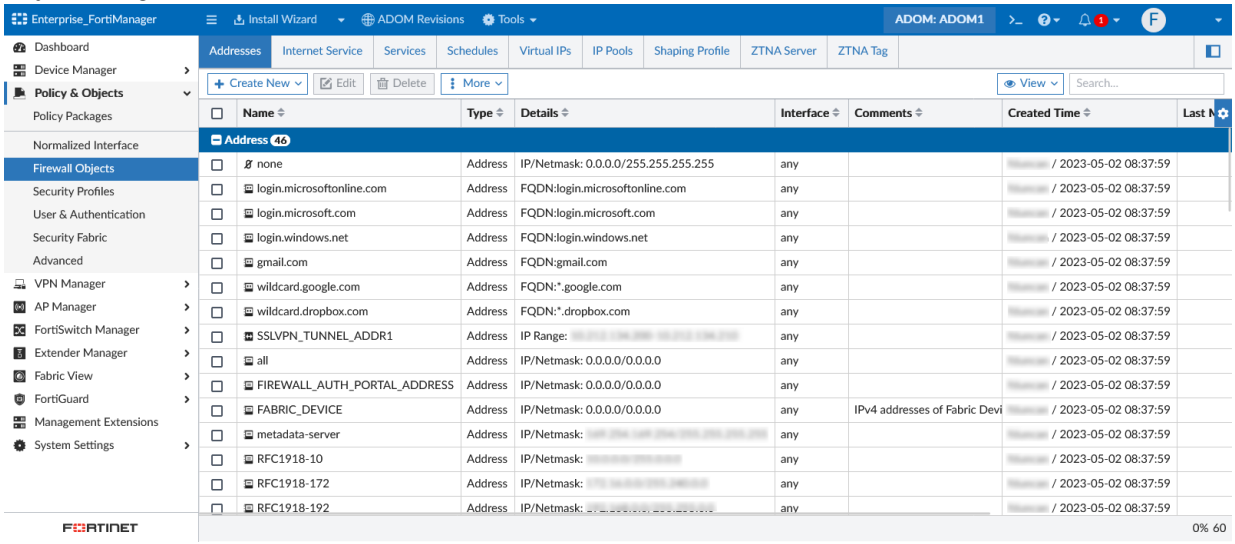

FMG-VM64
ADOM: FGT-72
admin
Dashboard
Device Manager
Policy & Objects
VPN Manager
AP Manager
FortiSwitch Manager
Extender Manager
FortiView
Log View
Fabric View
Incidents & Events
FortiGuard
Management Extensions
System Settings
Toggle Widget
Connectivity
Device Config Status
Policy Package Status
FortiAP Status
FortiSwitch Status
FortiExtender Status
Firmware Status
FortiGuard License Status
Hardware Vendor
Alert Message Console
Time
Message
Mar 2, 12:11:53
'admin' login failed from GUI(10.2.0.250), reason:Authentication failure. Please try again...
Mar 2, 12:08:56
fgfm connection to device FortiGate-81E-POE is up
Mar 2, 12:06:20
fgfm connection to device FortiGate-81E-POE is down
Mar 2, 11:47:46
Device FortiGate-81E-POE add succeeded
Mar 2, 11:47:21
fgfm connection to device FortiGate-81E-POE is up
Mar 2, 11:32:57
'admin' login failed from GUI(10.2.0.250), reason:Authentication failure. Please try again...
Mar 2, 11:31:48
Device FGT-27 add succeeded
Mar 2, 11:31:13
fgfm connection to device FGT-27 is up
Disk I/O
Insert Rate vs Receive Rate
License Information
Log Insert Lag Time
Log Receive Monitor
Receive Rate vs Forwarding Rate
System Information
System Resources
Unit Operation
1%
42%
6%
Average CPU Usage
Memory Usage
Disk Usage
More Details

Policy & Objects

- Policy Package configuration:

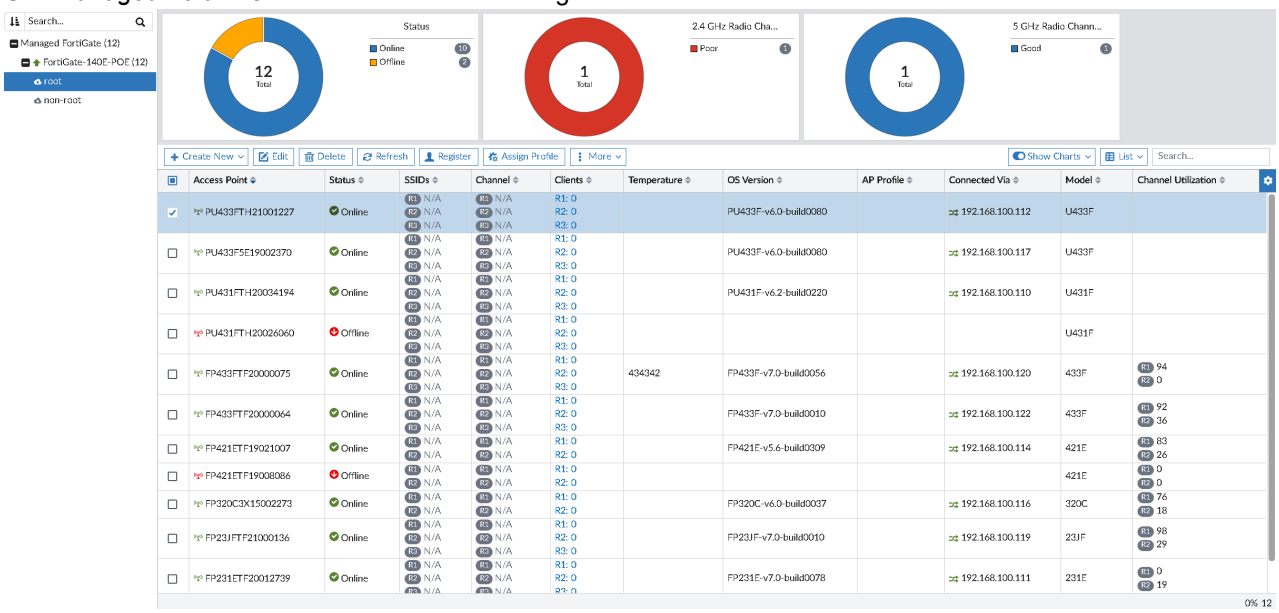


- Object configuration:

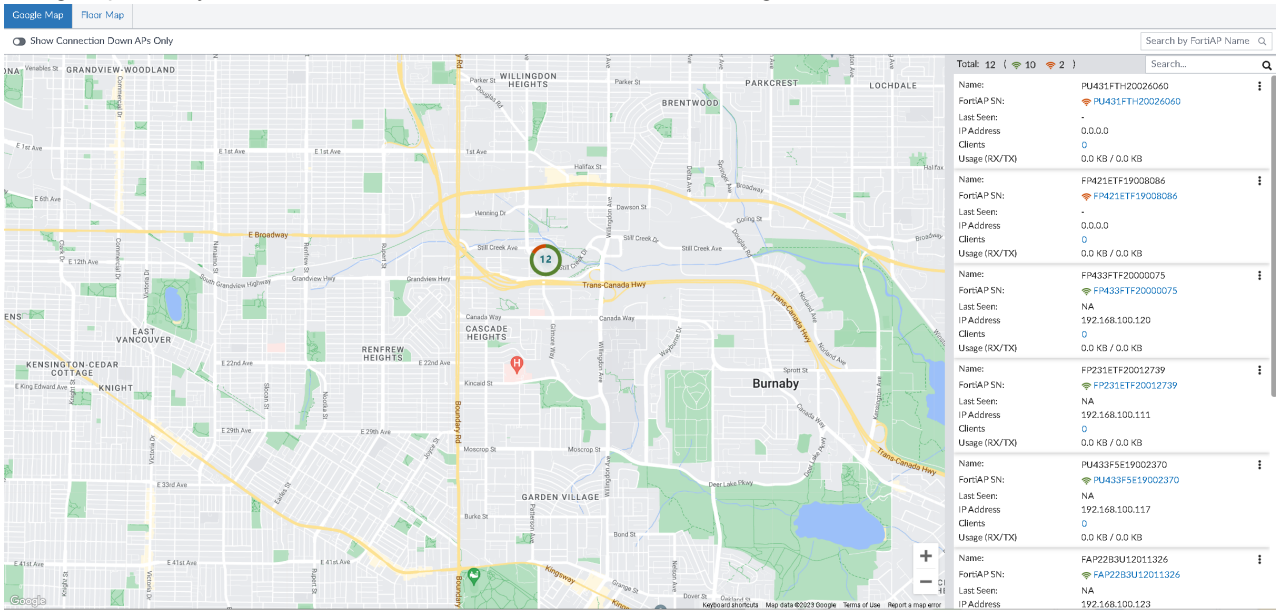


AP Manager

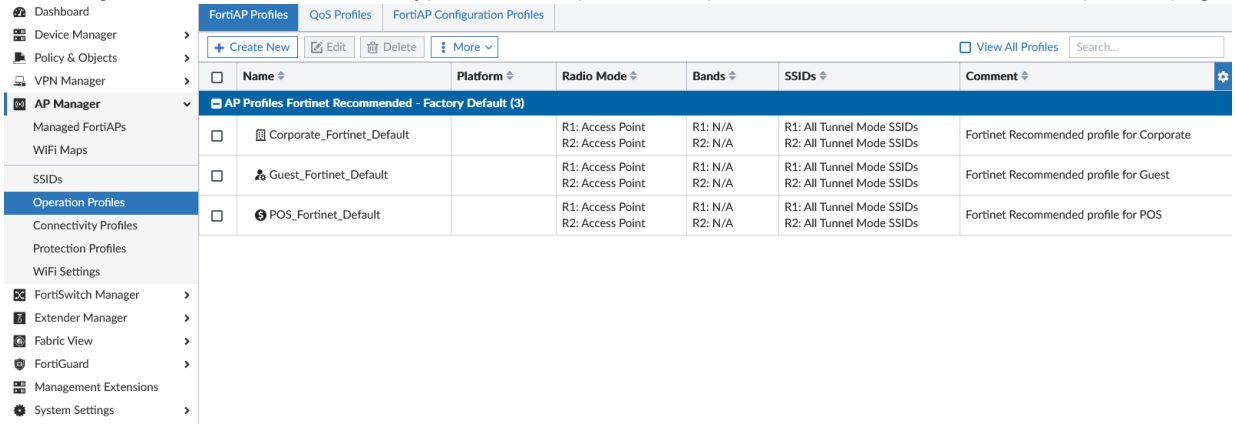
- Use *Managed FortiAPs* to view the status of managed FortiAP devices:



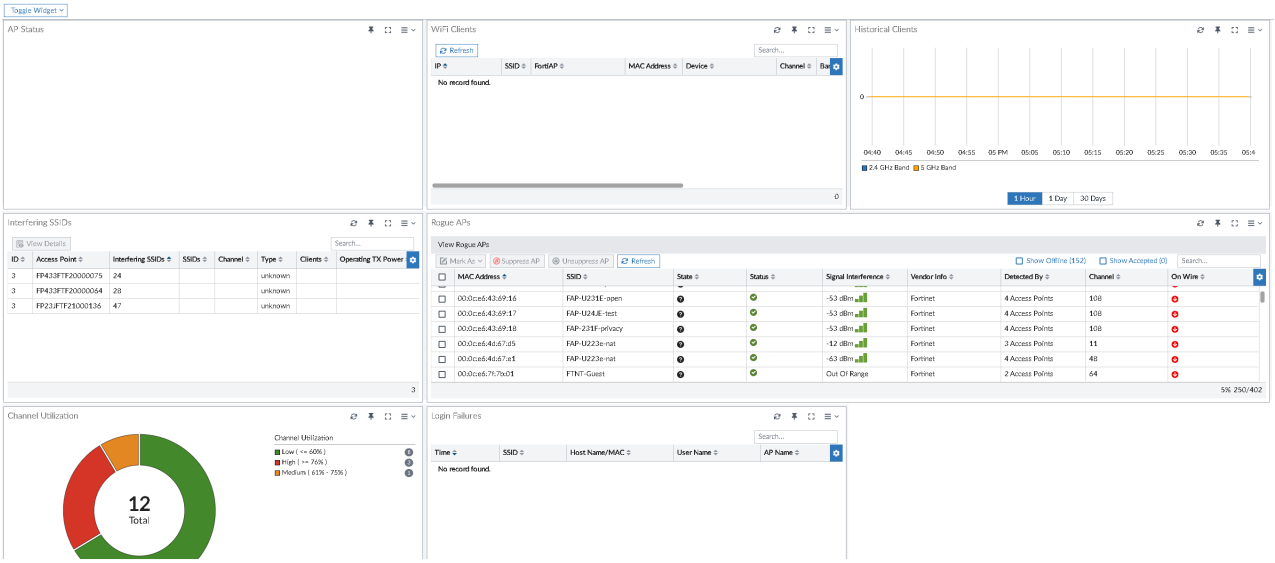
- Using *Map View*, you can check the location, info and status of managed FortiAP devices.



- Using *Operation Profiles*, *Connectivity Profiles*, and *Protection Profiles*, you can create different types of profiles and assign them to FortiAPs. Profile types, for example FortiAP profiles, are listed as tabs at the top of the page.

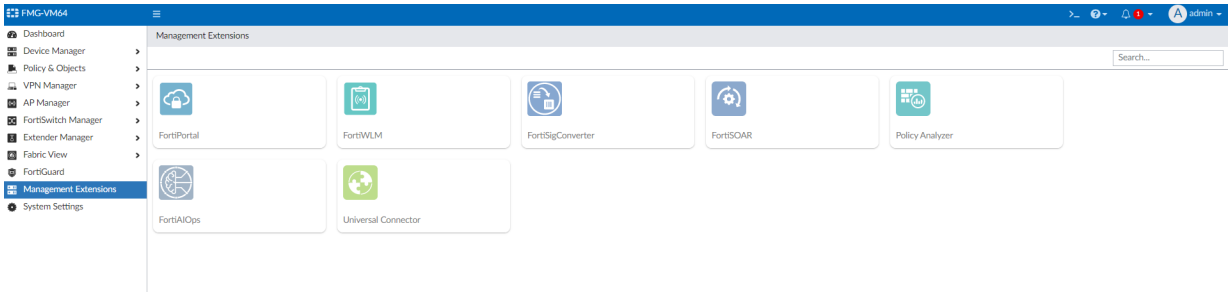


- Using *Managed FortiAPs* > *More* > *View Health Monitor*, you can see widgets related to the APs performance:



Management Extensions

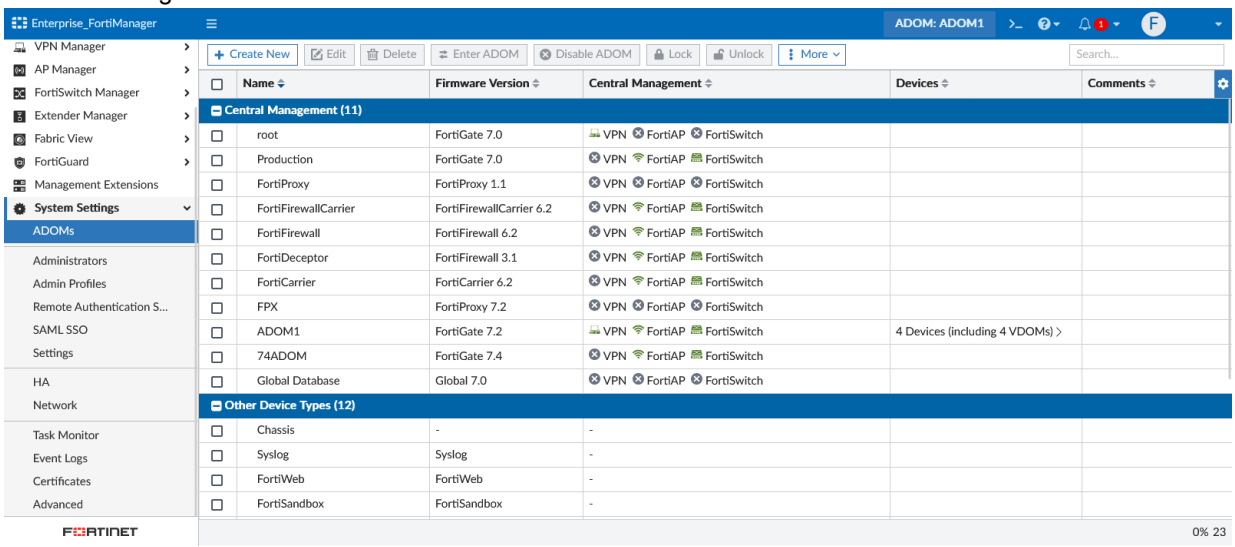
- Updated Management Extensions layout:



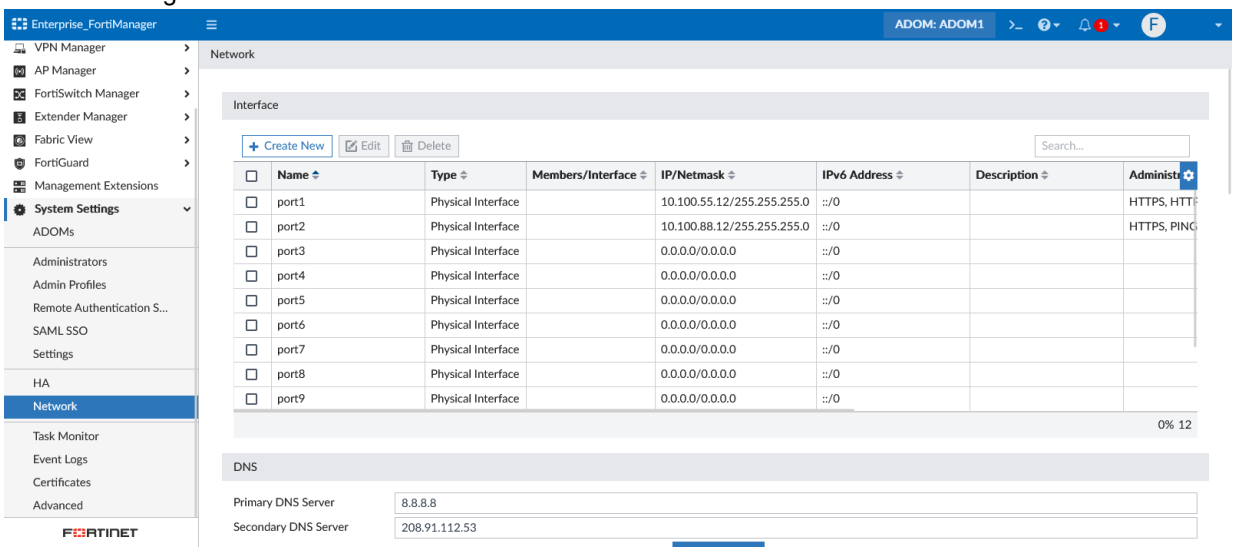
System Settings

System settings are available as tabs at the top of the system settings page.

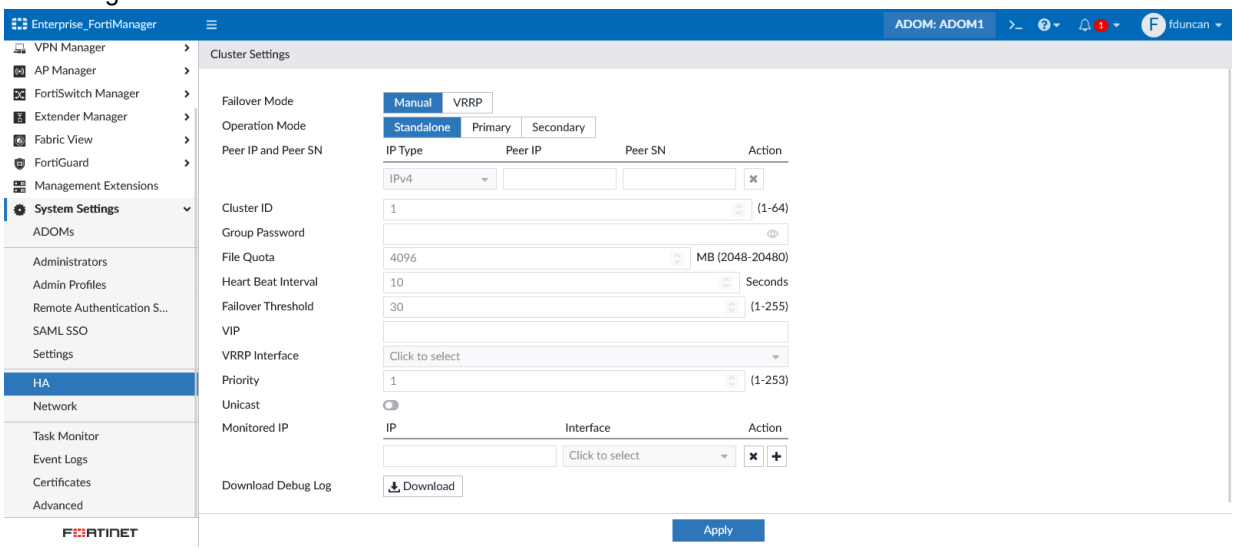
- ADOMs settings:



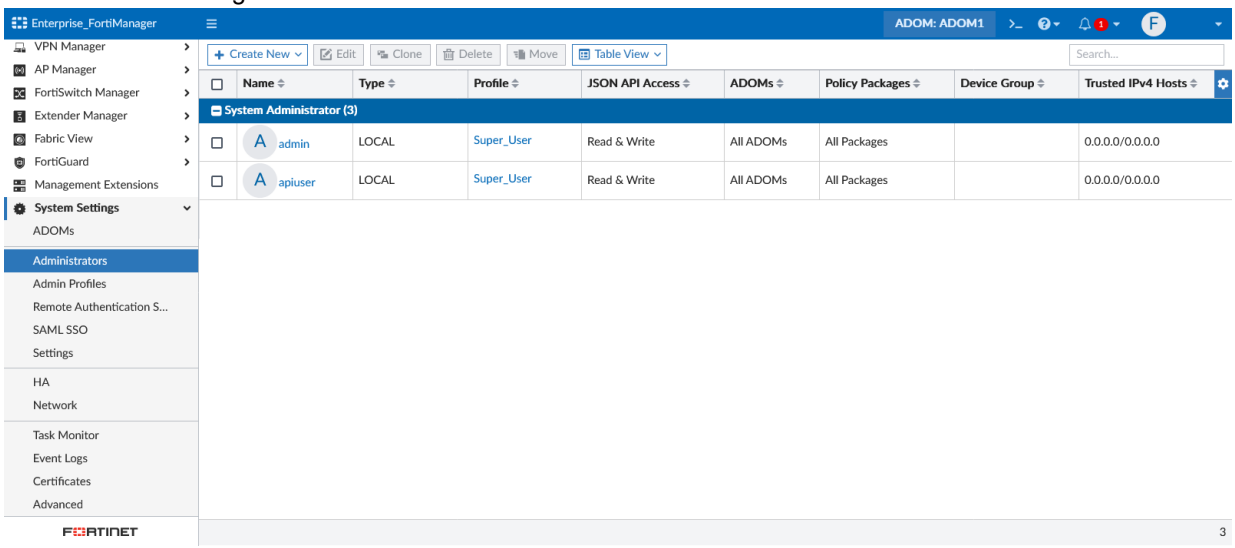
- Network settings:



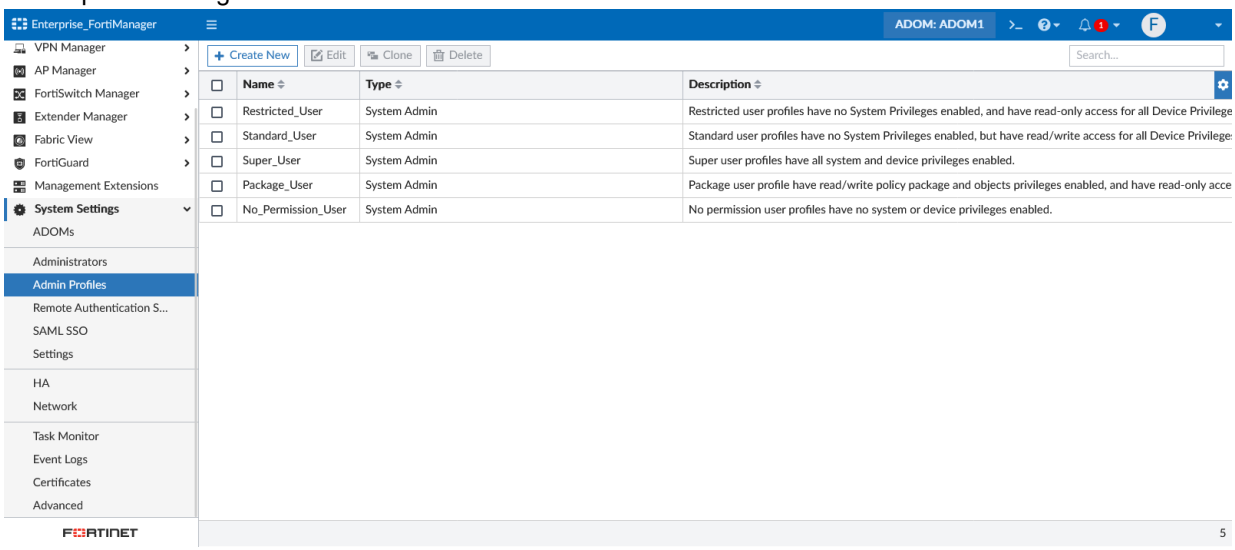
- HA settings:



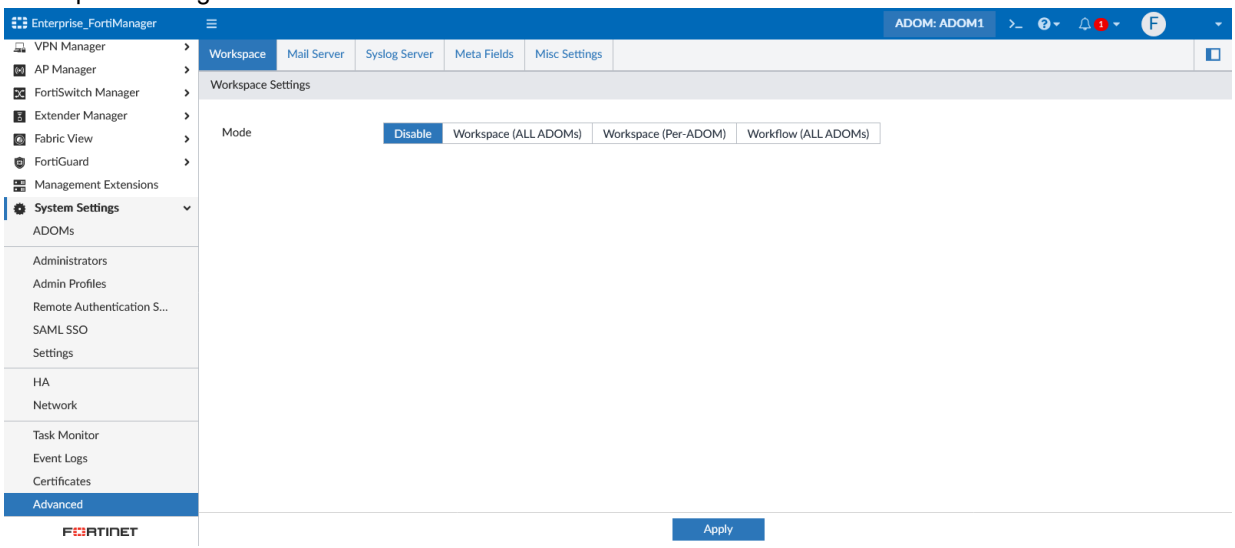
- Administrators settings:



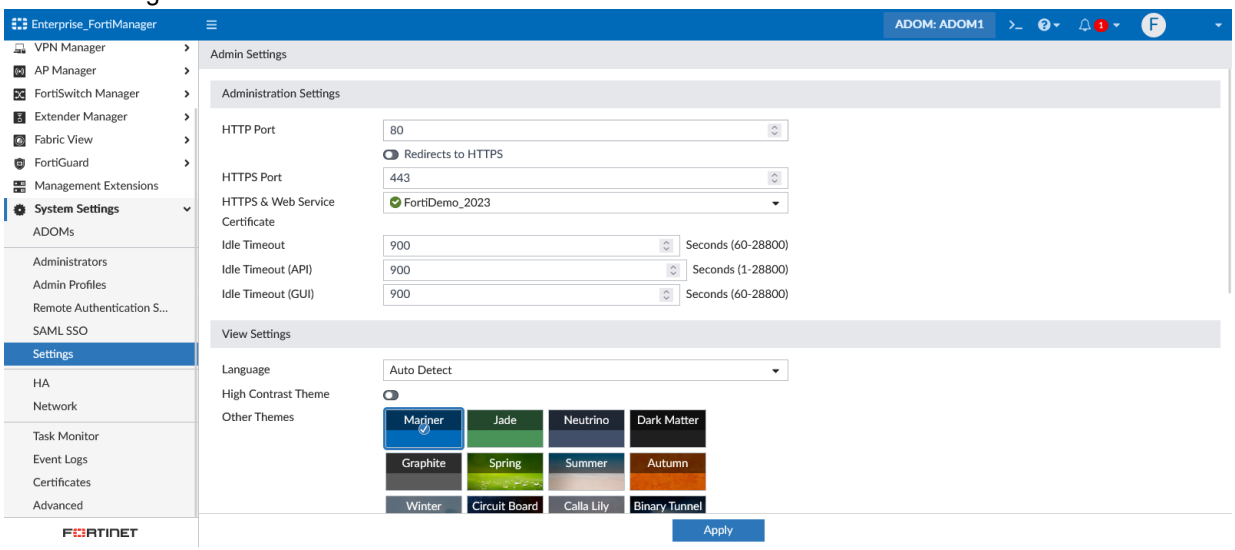
- Admin profile settings:



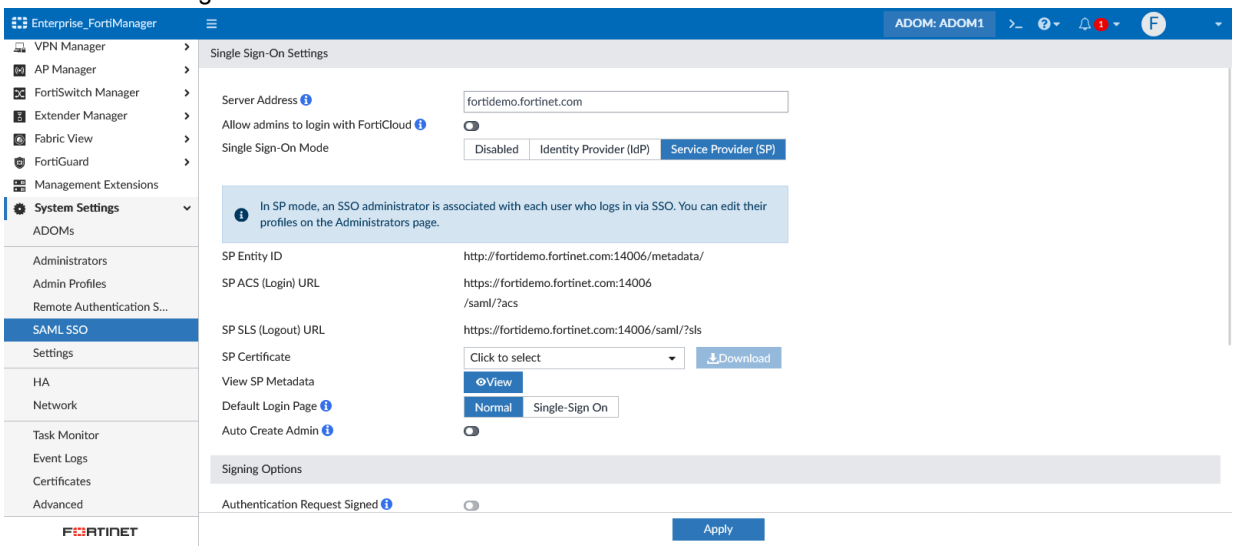
- Workspace settings:



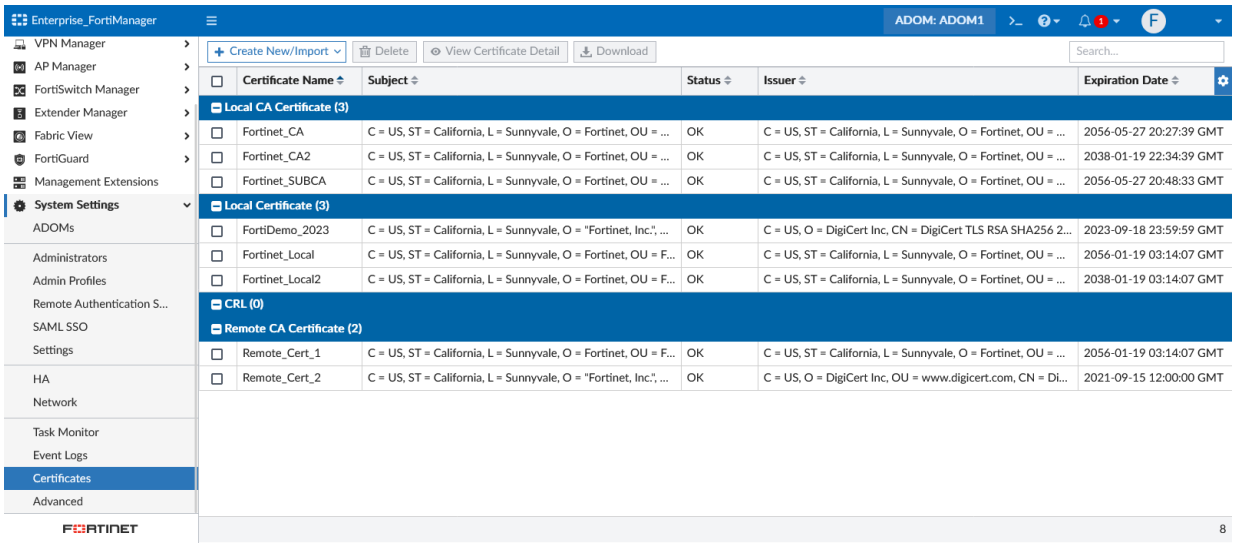
- Admin Settings:



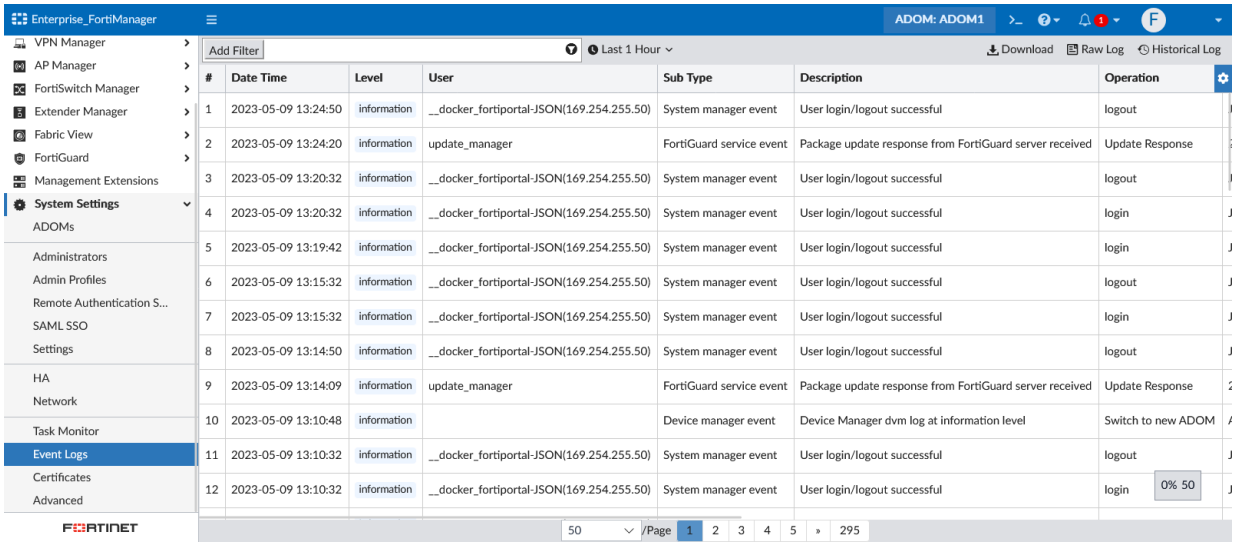
- SAML SSO settings:



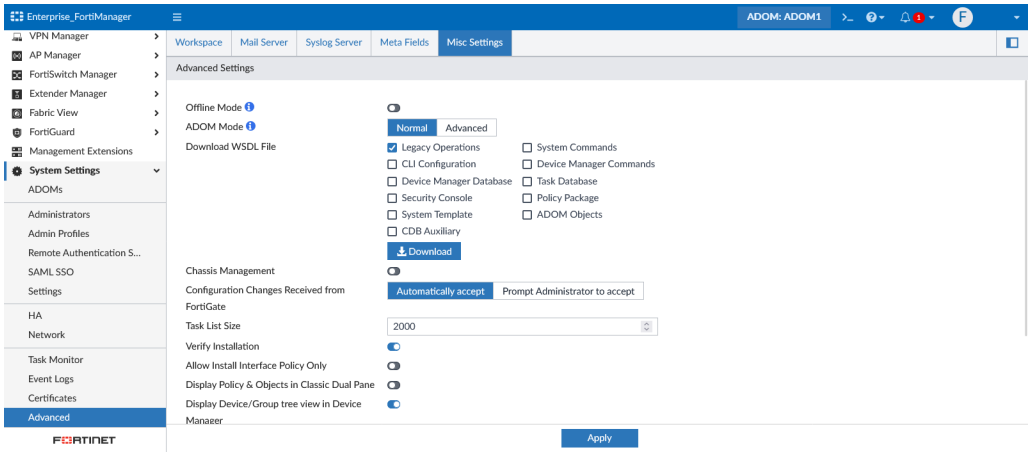
- Certificate settings:



- Event Log settings:



- Misc settings:



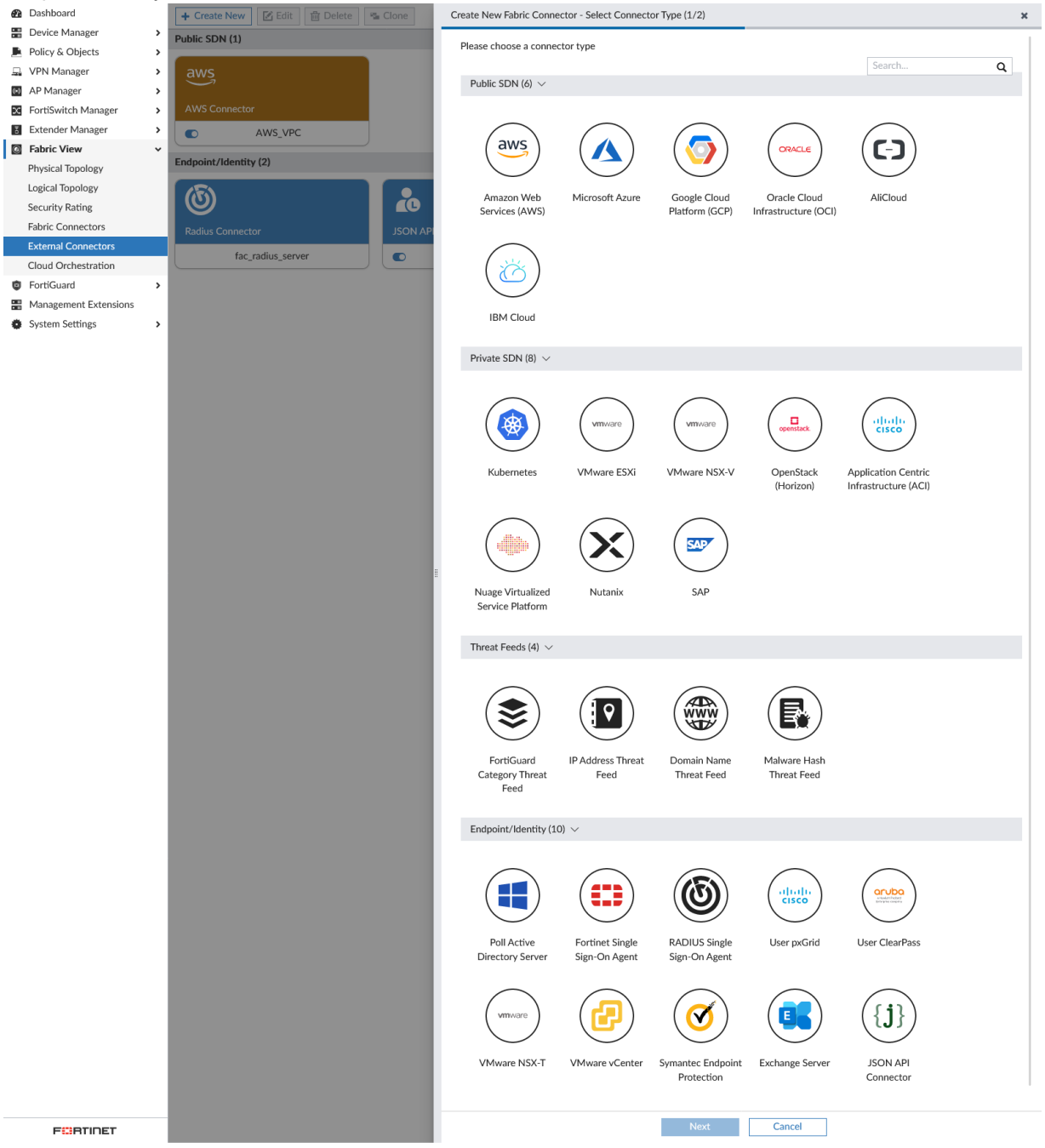
Fabric and External connector pages have been reorganized for an enhanced user experience

Fabric and External connector pages have been reorganized for an enhanced user experience, similar to the experience in FortiOS.

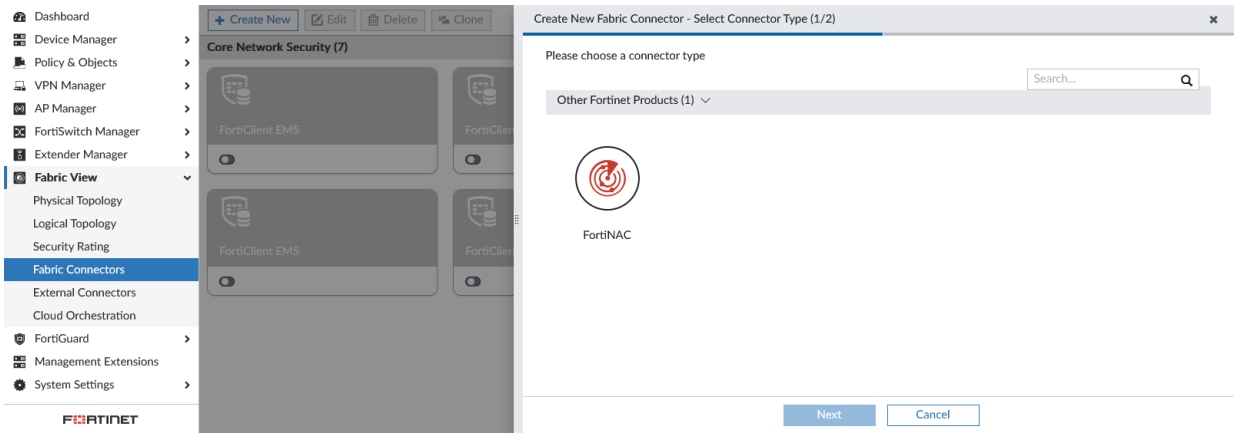
To view and configure connectors in Fabric View:

1. Go to *Fabric View* . The *Fabric Connectors* and *External Connectors* pages are available in the tree menu under *Fabric View*.
   The following connector types have been moved into the *External Connectors* menu.
   - Public SDN
   - Private SDN
   - Threat Feeds

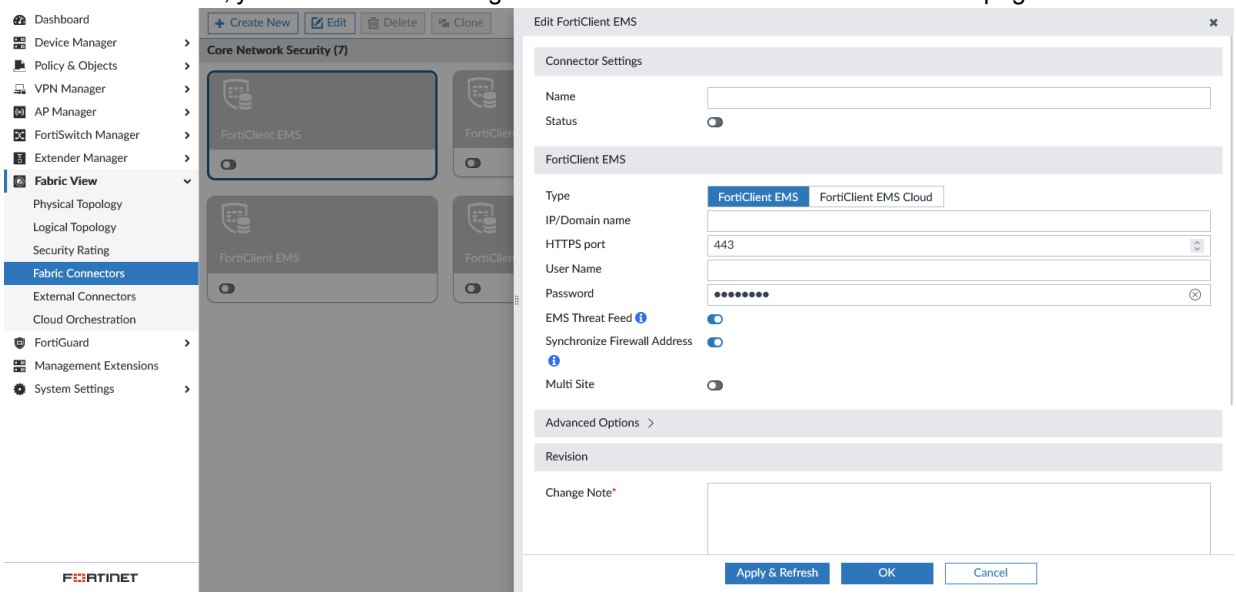
- Endpoint/Identity



The *FortiClient EMS* and *FortiNAC* connectors have been moved into the *Fabric Connectors* menu.



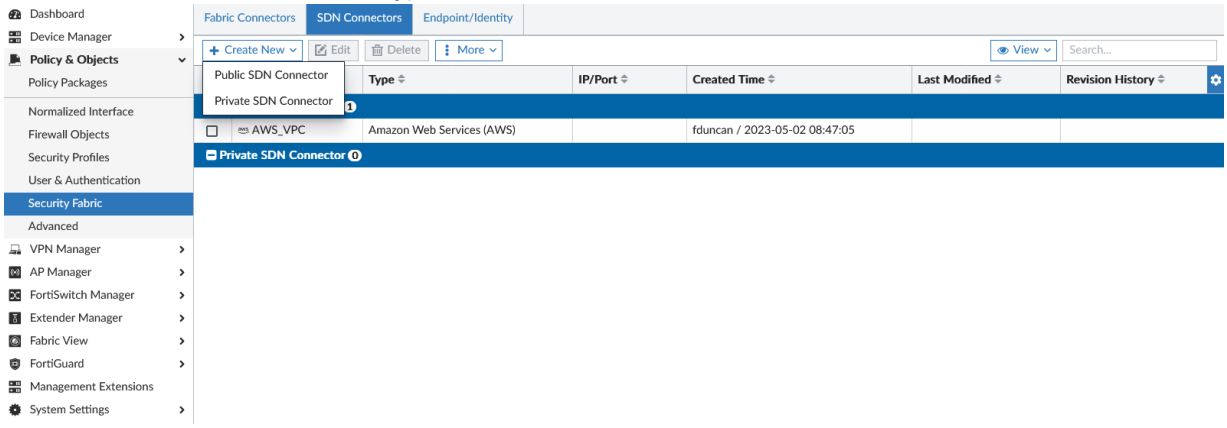
2. Click *Create New* to create a new connector while in the *Fabric Connectors* or *External Connectors* view. For FortiClient EMS, you can edit the existing EMS connectors on the *Fabric Connectors* page.



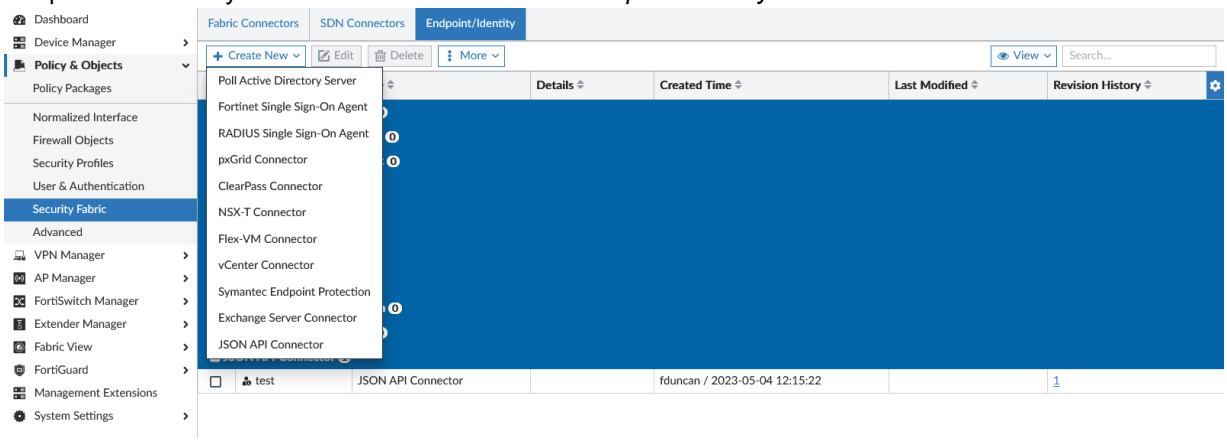
To view and configure connectors in Policy & Objects:

1. Go to *Policy & Objects* > *Security Fabric*.
   The *Fabric Connectors*, *SDN Connectors*, and *Endpoint/Identity* menus are available as tabs.

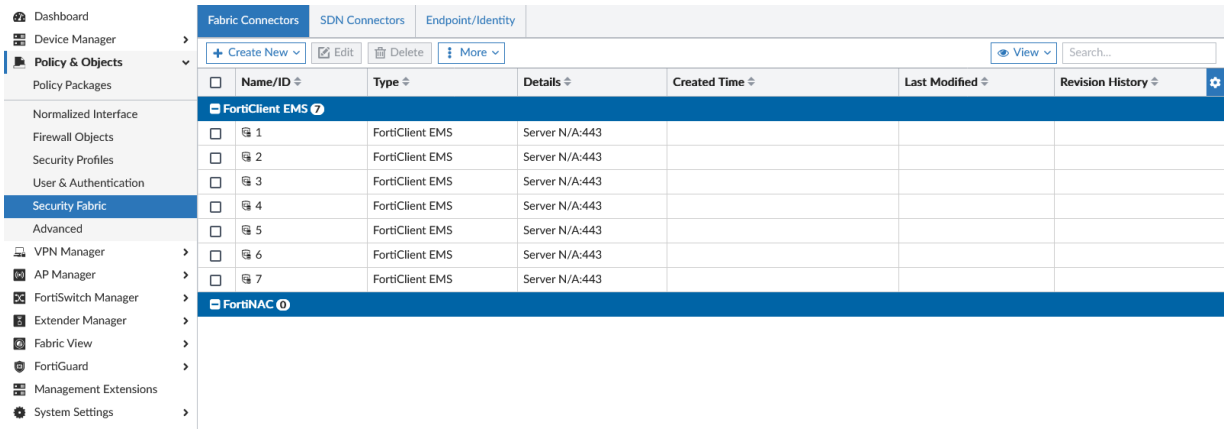
- Public and Private SDN connector types are included in the *SDN Connectors* tab.



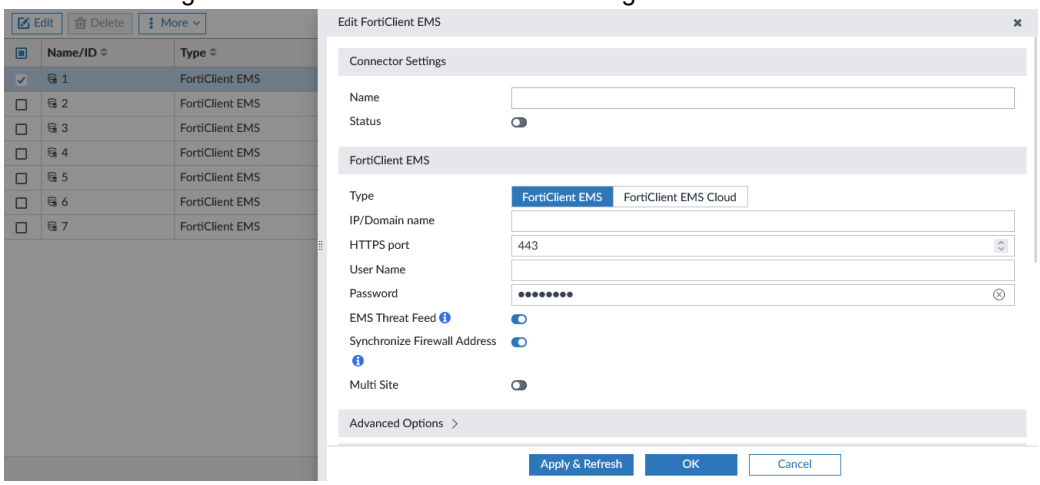
- Endpoint and identity connectors are included in the *Endpoint/Identity* tab.



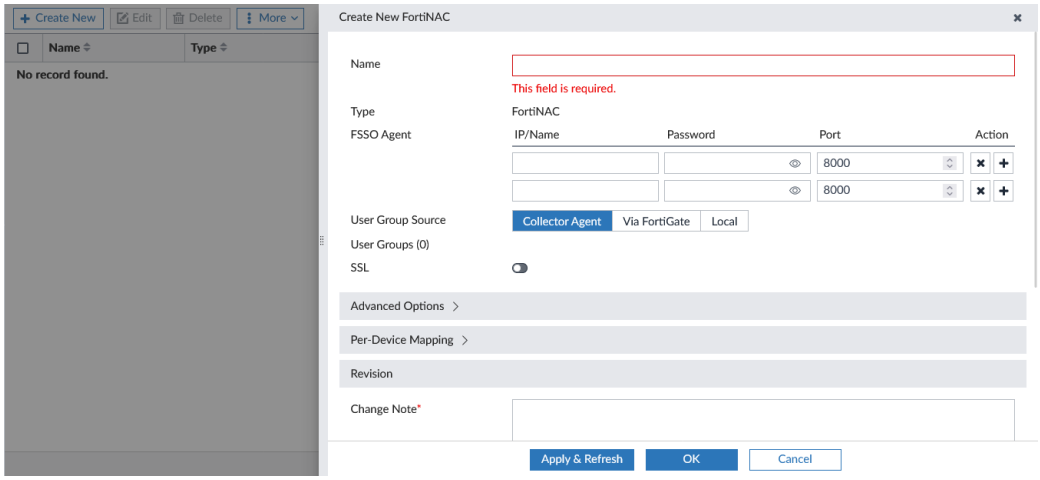
- FortiClient EMS and FortiNAC connectors are included in the *Fabric Connectors* tab.



2. To configure FortiClient EMS connectors, navigate to *Policy & Objects* > *Security Fabric* > *Fabric Connectors*, and select an existing EMS connector to edit and make changes to it.



3. To configure FortiNAC connectors, navigate to *Policy & Objects* > *Security Fabric* > *Fabric Connectors* and click *Create New*.



FortiManager connector relay to AWS will proxy all individual FortiGate requests

This information is also available in the FortiManager 7.4 Administration Guide:

- Using FortiManager as an SDN proxy for AWS connectors

FortiManager connector relay to AWS will proxy all individual FortiGate requests.

This feature can only be configured using the CLI.

To configure the FortiManager connector relay to AWS:

1. In the FortiGate CLI, create the proxy object:
   config system sdn-proxy **<---- new object**
   ```
   edit <sdn-proxy name>
      set type fortimanager
      set server <server address>
      set username <username">
      set password <password>
   next
   end
   ```
2. In the FortiGate CLI, configure the SDN connector to use the proxy.
   ```
   config system sdn-connector
      edit "aws1"
         set proxy <sdn-proxy name> <---- new property
         set use-metadata-iam disable
         set access-key <access>
         set secret-key <secret>
         set region "us-west-2"
      next
   end
   ```
3. On the FortiManager, you can manage the SDN proxy daemon with the following commands in the CLI:
   - The *sdnproxy* daemon is able to restart by using the `diagnose test application sdnproxyd <xx>` command where `xx` is the level of debug.
   - The *sdnproxy* daemon shows debug logs using the `diagose debug application sdnproxy <xx>` command where `xx` is the level of debug.

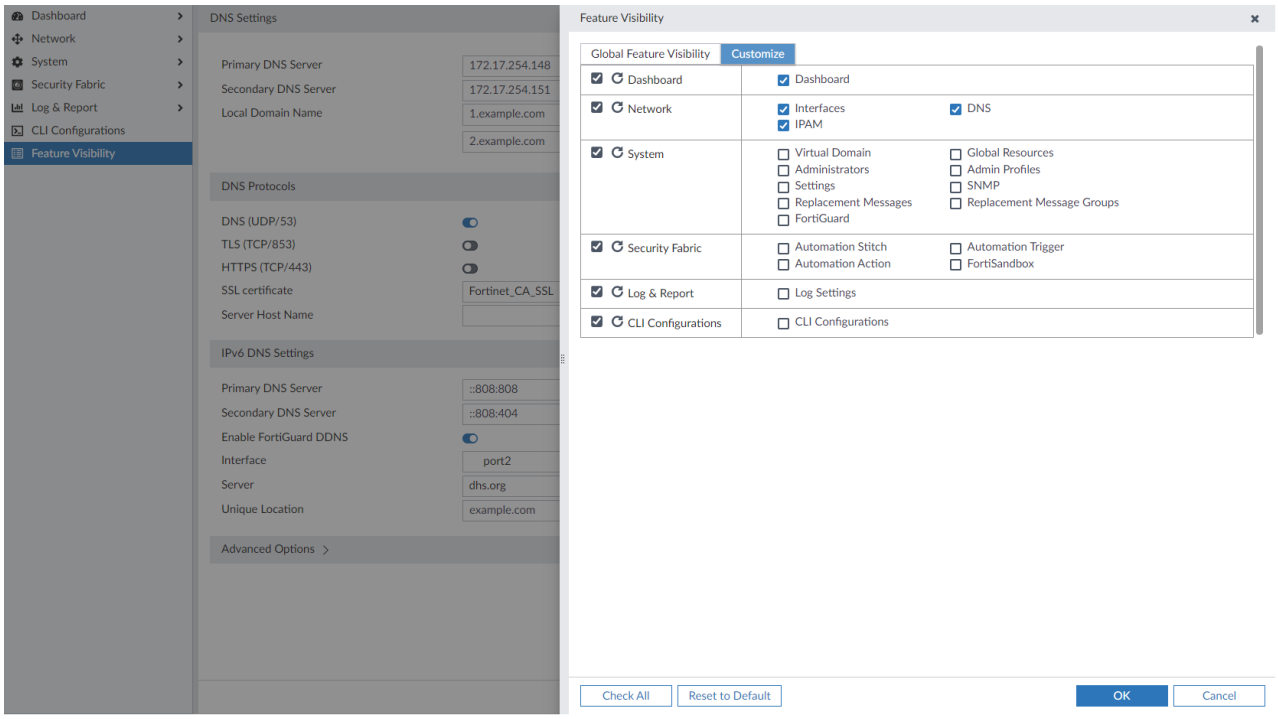
FortiManager key areas have been reorganized to enhance user experience

FortiManager key areas have been reorganized to enhance user experience, similar to FortiOS.

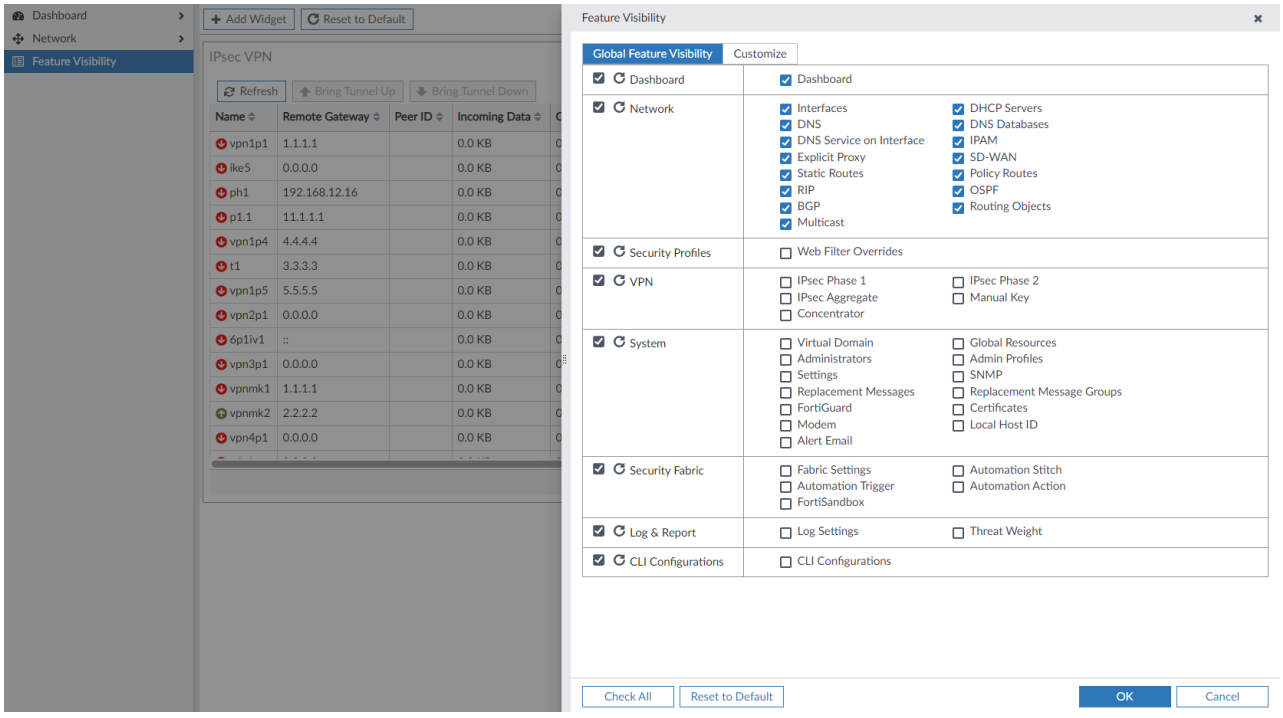
This topic includes the following sections:

Device Manager

- In the *Device Manager* device database, you can use *Feature Visibility* to enable network related features under the *Network* tree in the VDOM level.

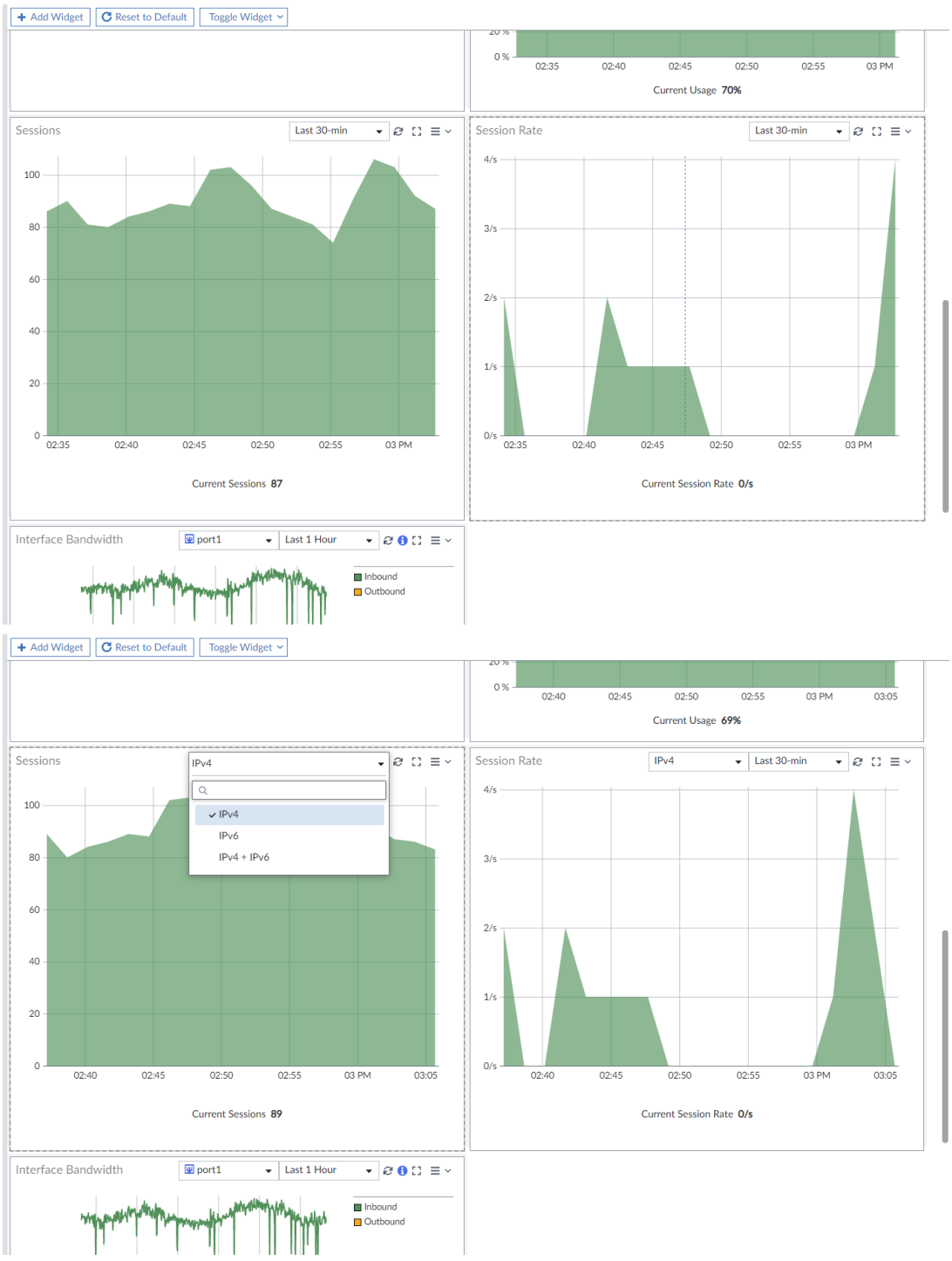


- Enable network features in the *Global Feature Visibility* menu.



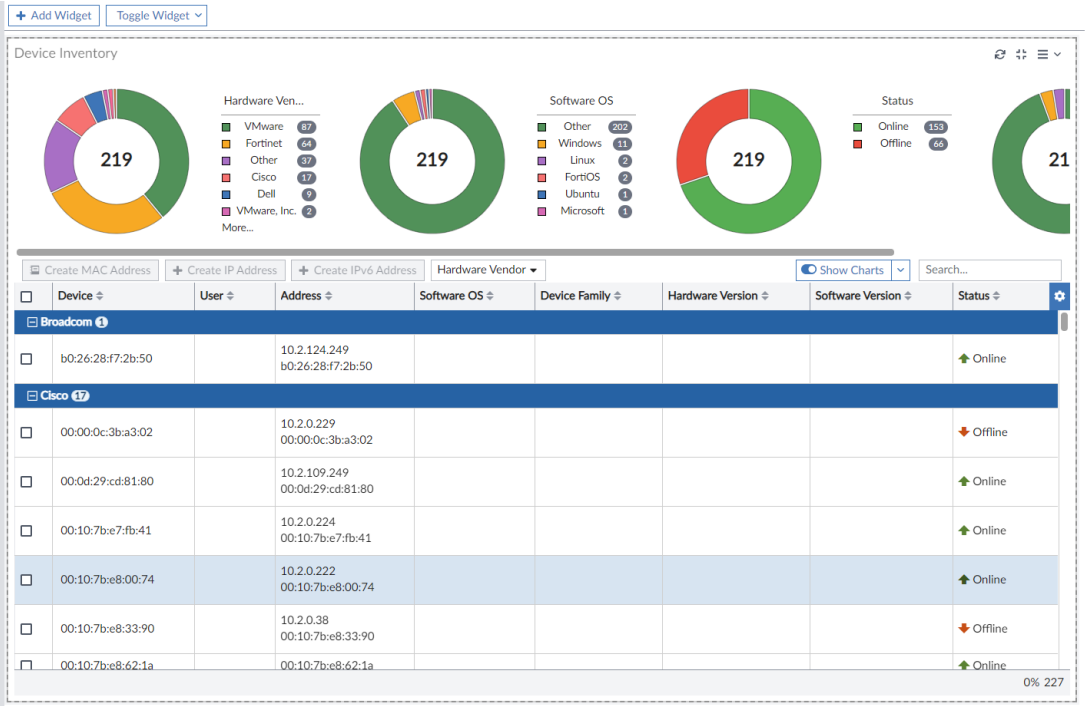
- Network related device configuration features are moved under the *Network* tree group. The following features have been moved from the *Router* and *System* menu to the new *Network* menu.
  - Interfaces
  - DHCP Servers
  - SD-WAN
  - DNS (Global tree feature)

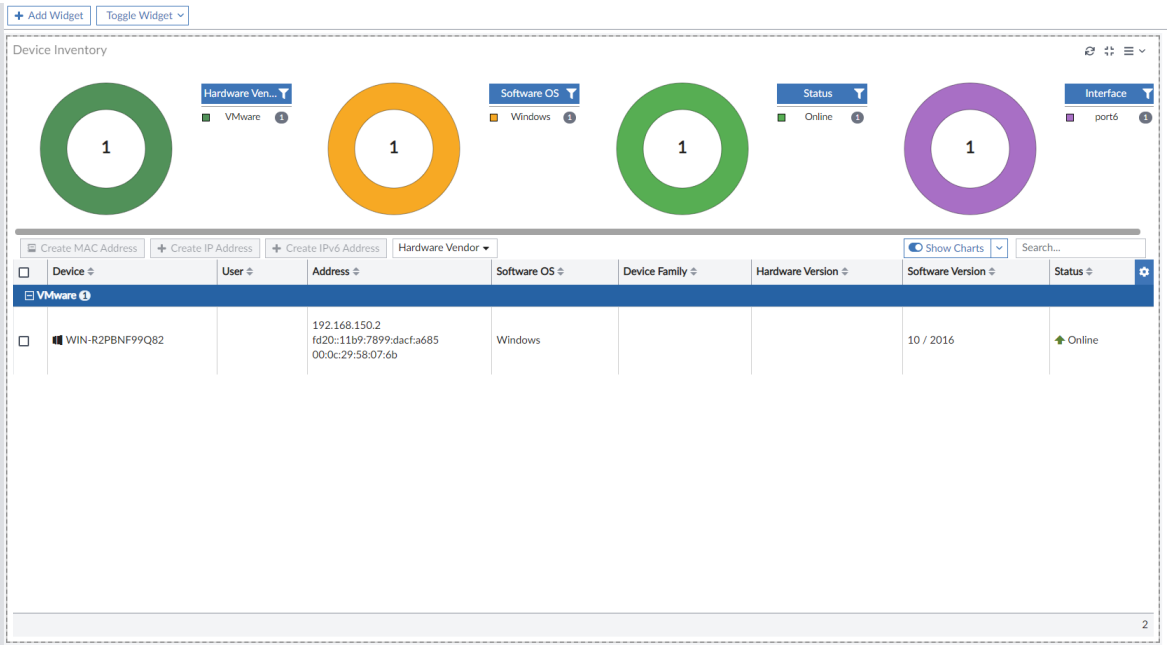
    - DNS Database
    - DNS Service on Interface
    - IPAM (Global tree feature)
    - Explicit Proxy
    - Static Routes
    - Policy Routes
    - RIP
    - OSPF
    - BGP
    - Routing Objects
    - Multicast
- The following device dashboard widgets are new or improved:
    - *Session* and *Session Rate*:
        - Changed from a line chart to an area chart.
        - Displays a dropdown list when IPv6 is enabled on FortiGate (options include: IPV4, IPV6, and IPV4 + IPV6), and displays the relevant chart based on the selected option.



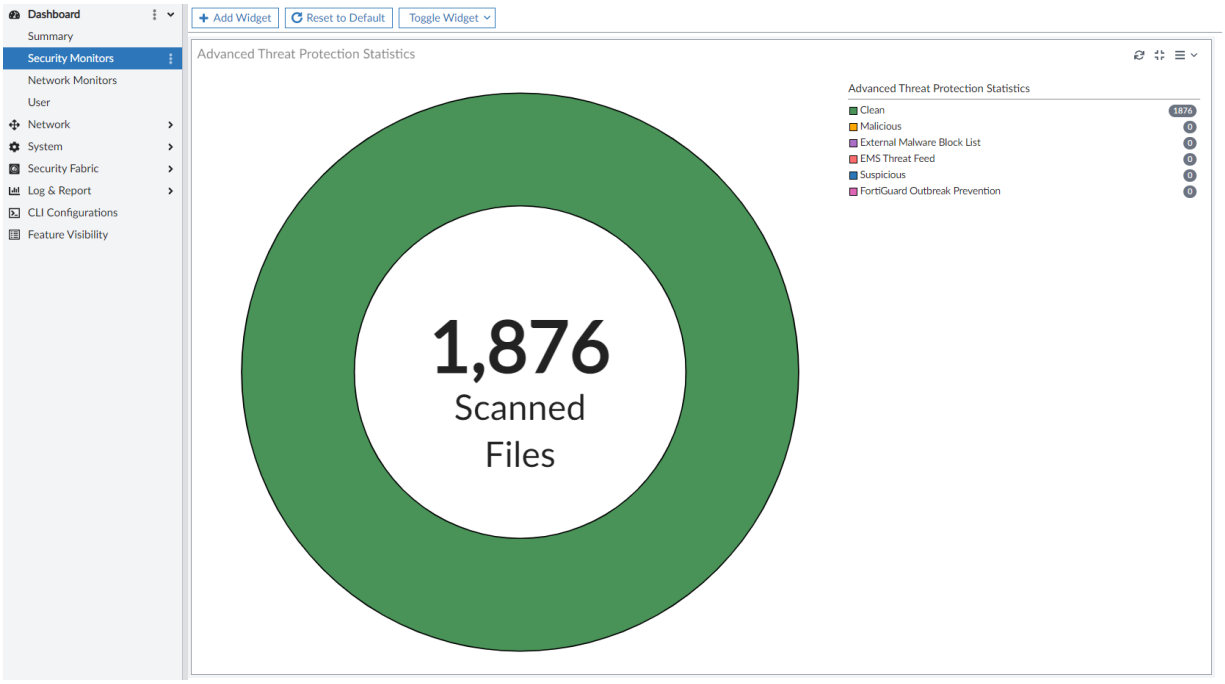
- *Device Inventory*:
  - The widget has added donut charts.
  - You can group and display the results by the hardware vendor or software OS.

- You can filter the result by the hardware vendor, software OS, status and interface.

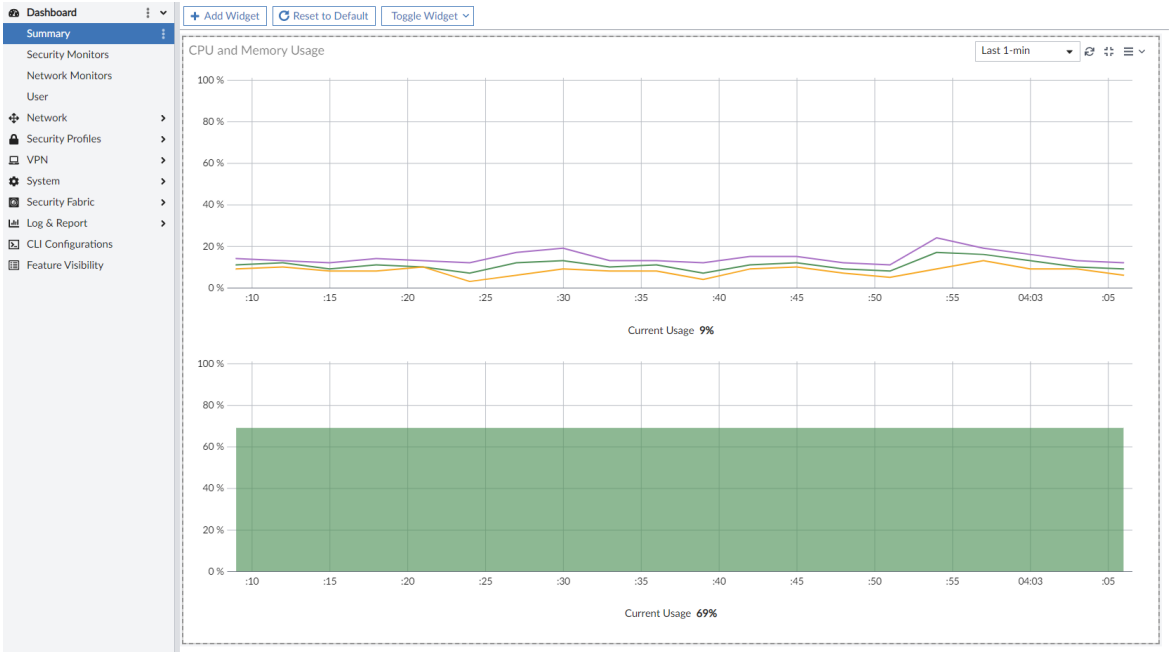




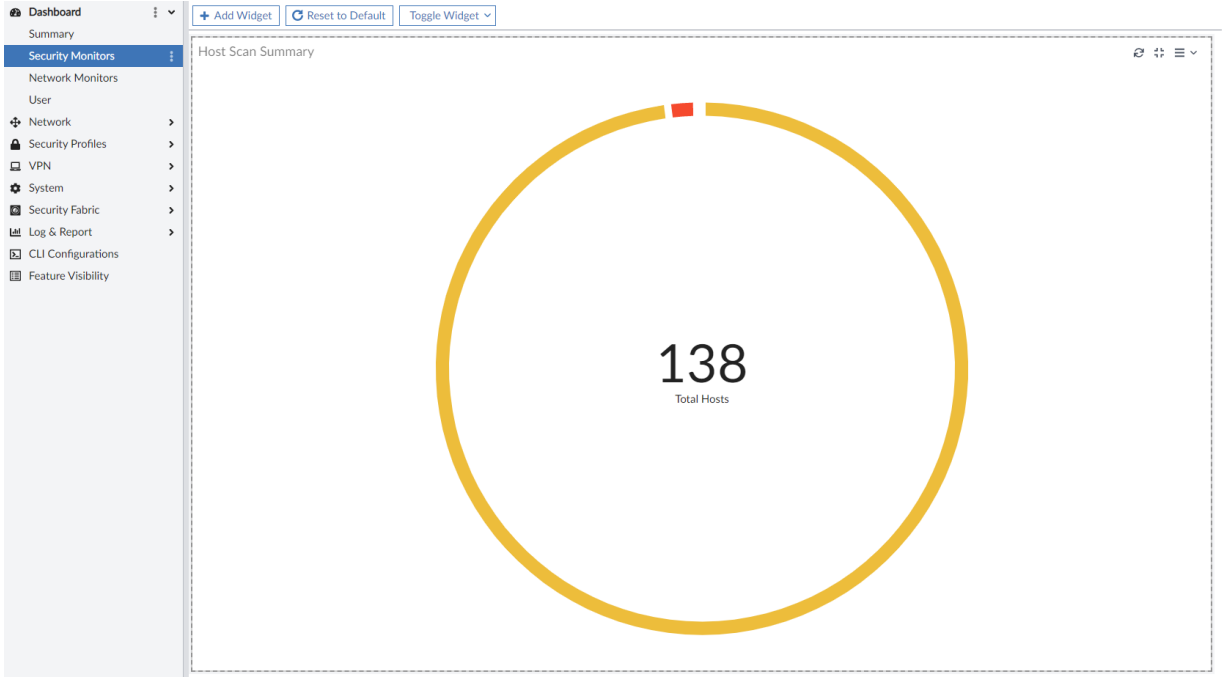
- *Advanced Host Scan:*



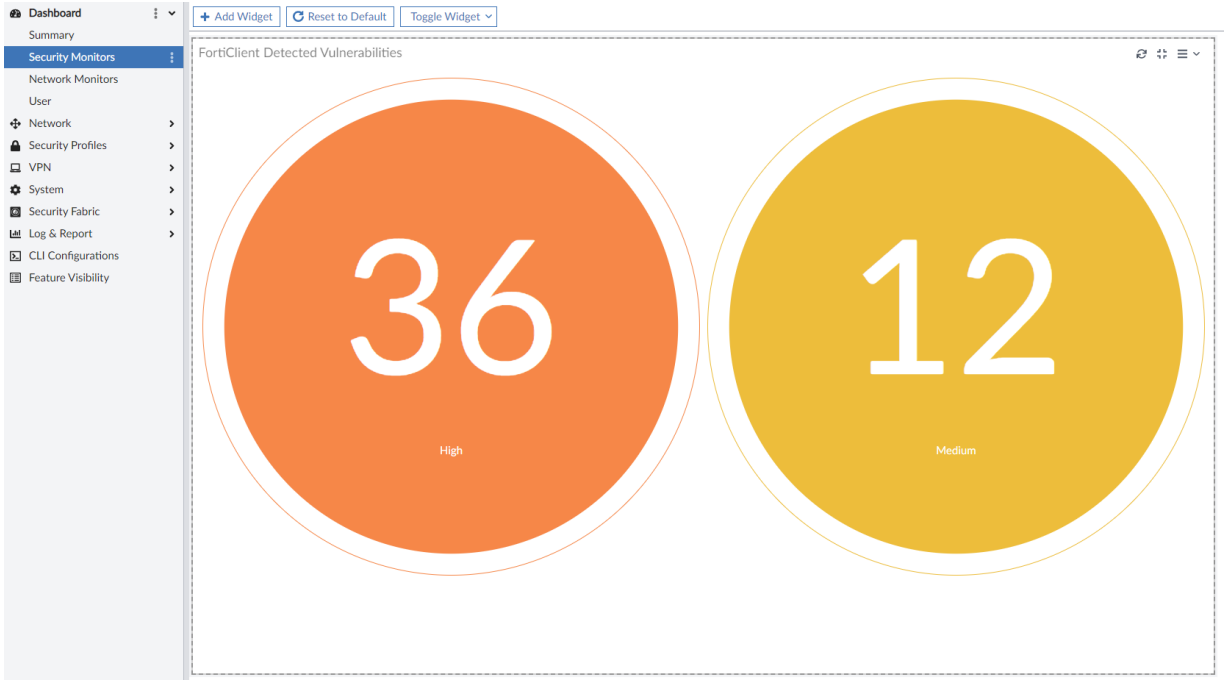
- *CPU and Memory Usage*:
  - The memory chart has been changed from a line chart to an area chart.
  - The CPU chart shows the usage of each CPU for multi-CPU devices.



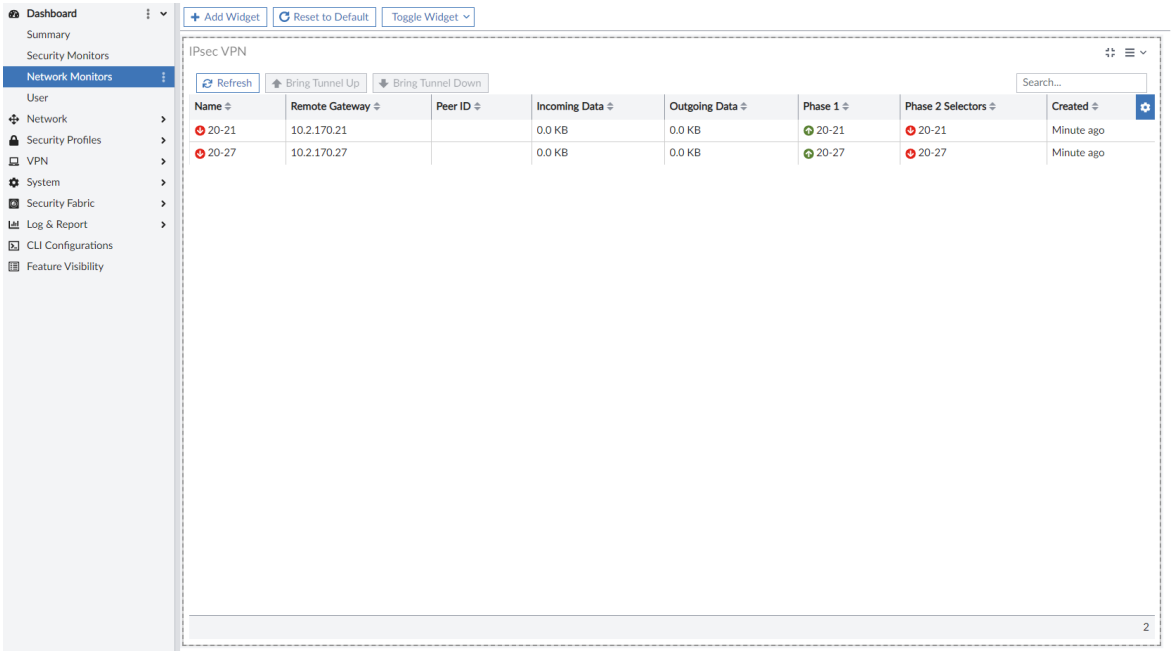
- *Host Scan Summary:*

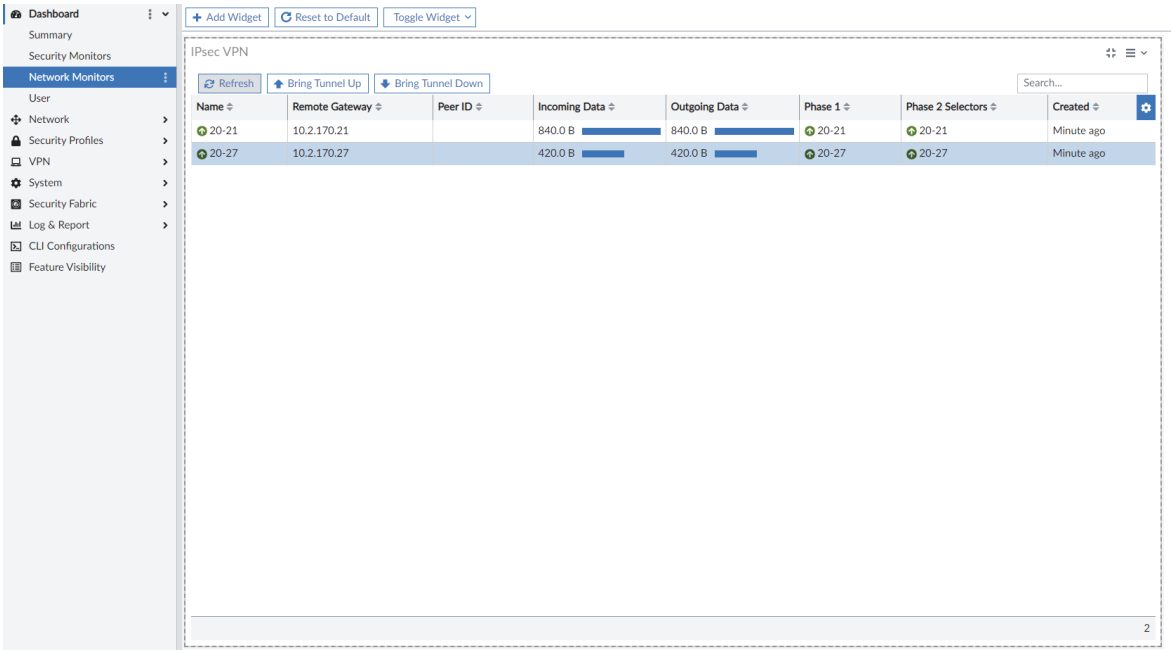


- *FortiClient Detected Vulnerabilities*:



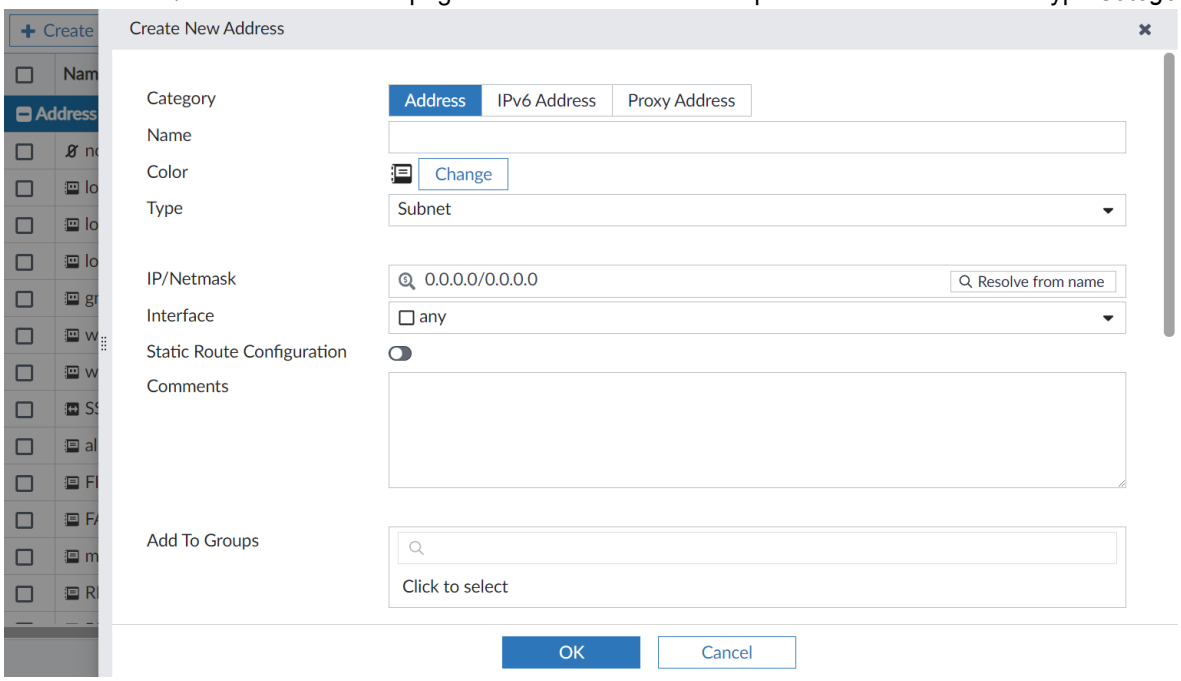
- *IPSEC VPN Widget*:
  - The icon is red when the tunnel is down.
  - The widget shows progress bars for incoming and outgoing traffic.



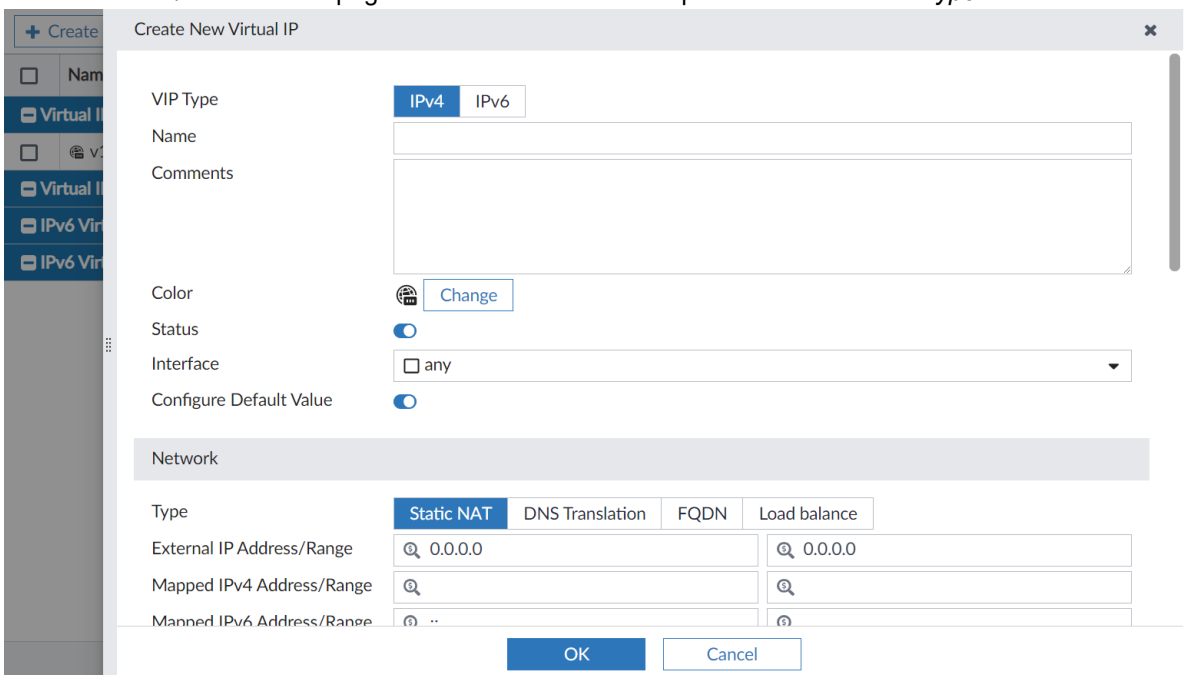


Firewall Objects

- The create new/edit firewall address page uses tabs instead of a dropdown list for the address type *Category*.

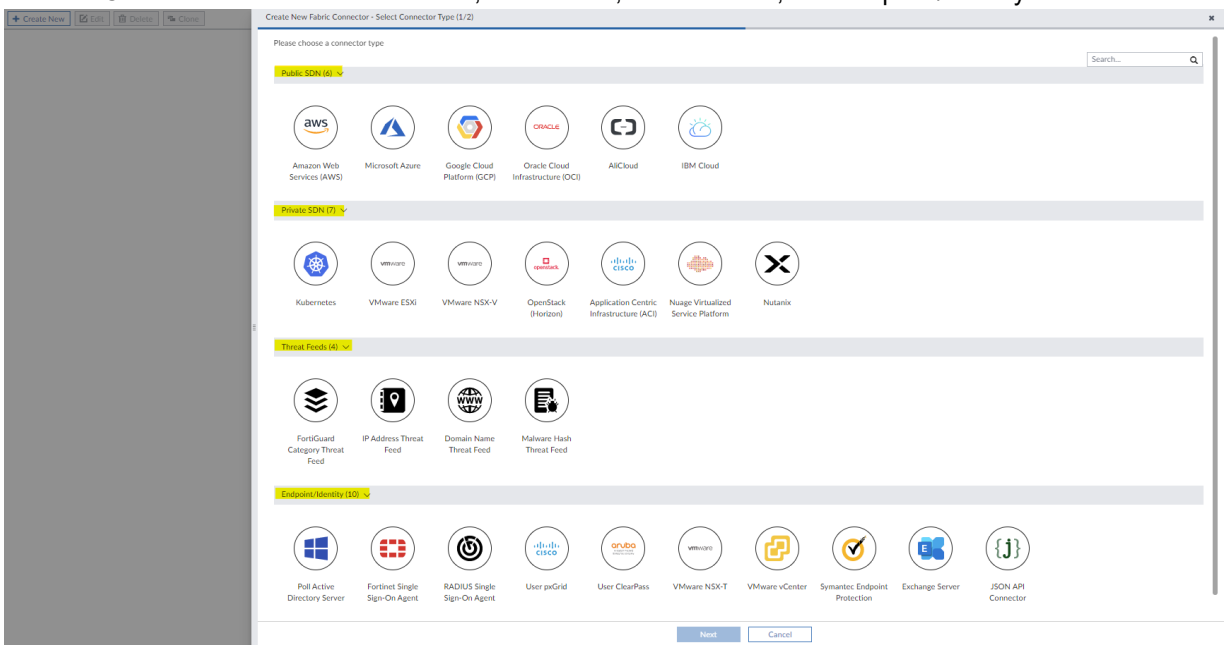


- The create new/edit Virtual IP page uses tabs instead of a dropdown list for the *VIP Type*.

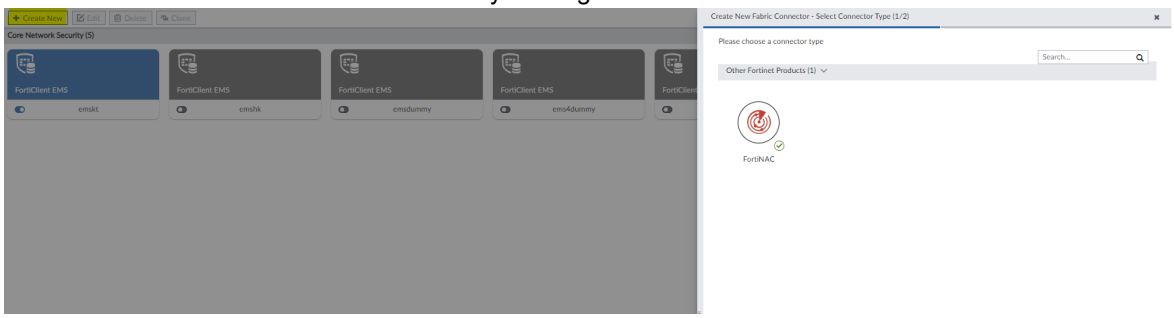


Fabric Connector

- Fabric connectors are reorganized by *Fabric Connectors* and *External Connectors*.
  - External Connectors includes Private SDN, Public SDN, Threat Feeds, and Endpoint/Identity.



  - Fabric Connectors include EMS and FortiNAC connectors.
    - You can create a new FortiNAC connector by clicking *Create New*.

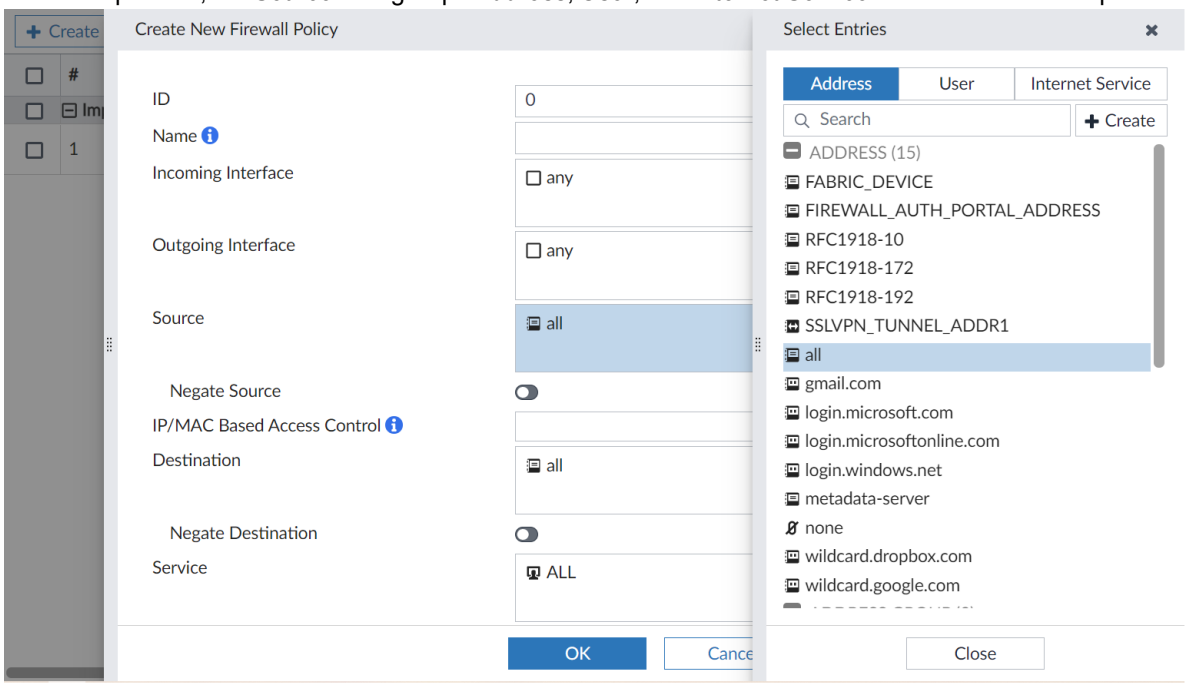


    - To configure an EMS connector, edit one of the existing default EMS connectors.

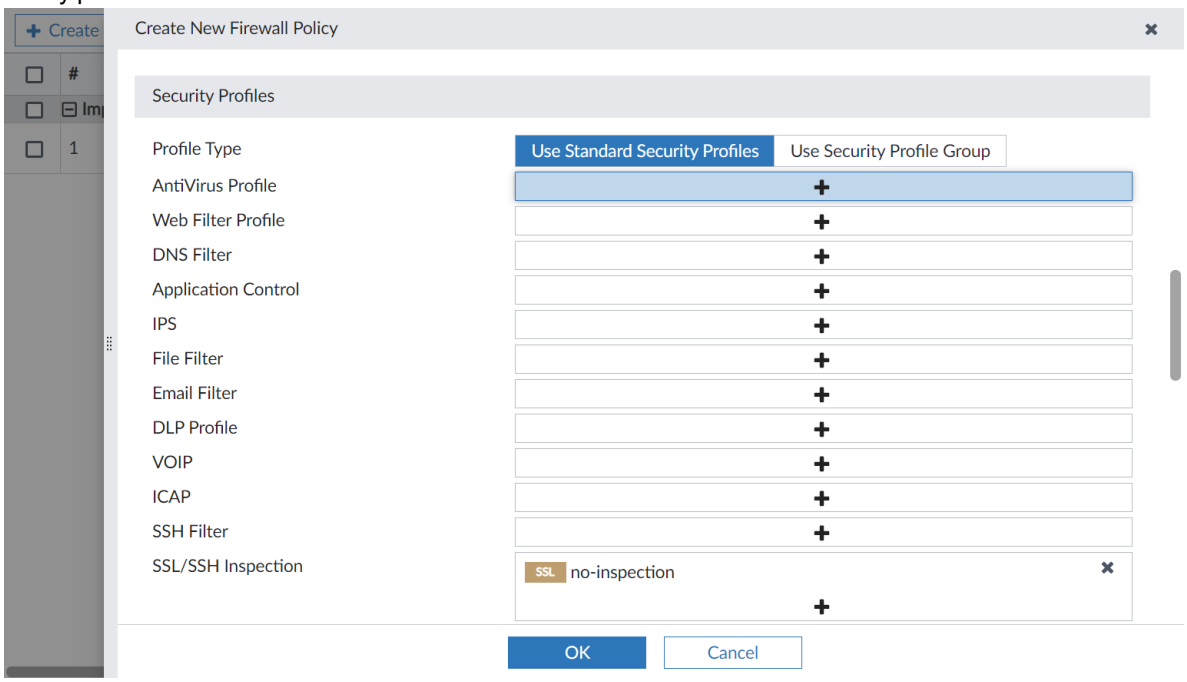
    - Users can also create fabric connectors from *Policy & Objects* by going to *Policy & Objects* > *Security Fabric* and selecting the *Fabric Connectors*, *SDN Connectors*, or *Endpoint/Identity* tabs.

Firewall Policies

- In firewall policies, the *Source* field groups *Address*, *User*, and *Internet Service* into one field with separate tabs.

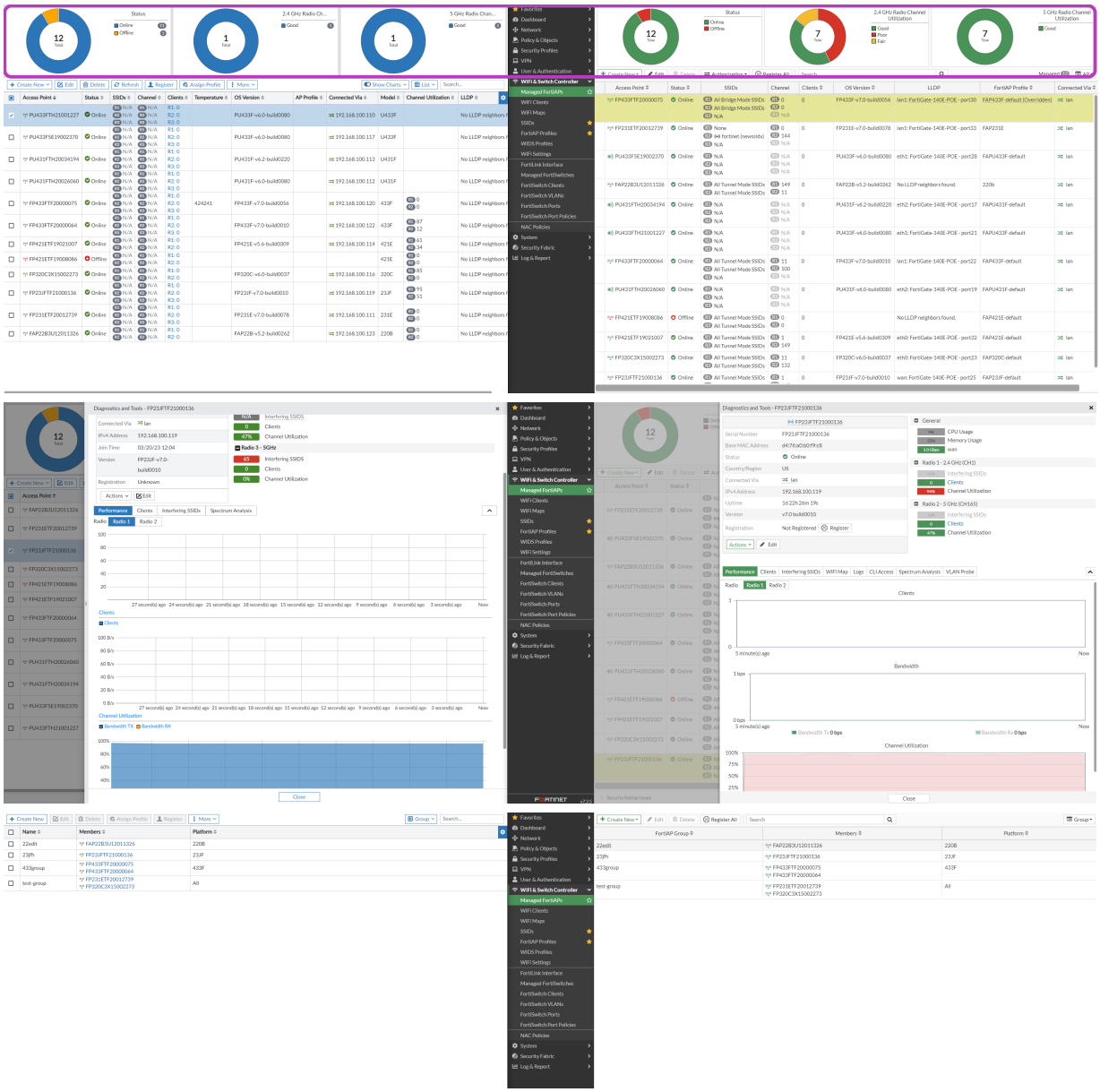


- Policy profiles have been made easier to find.

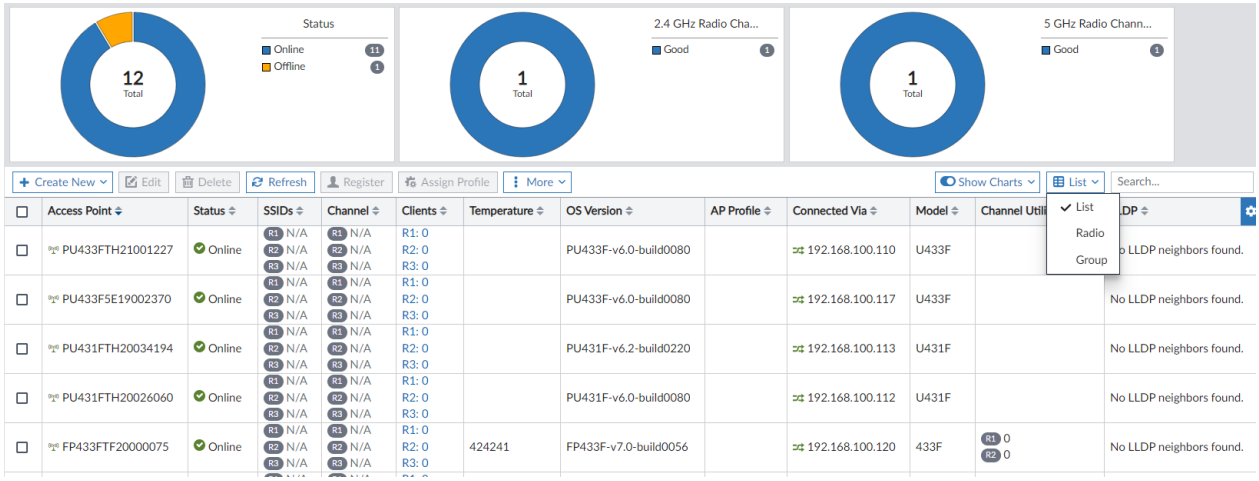


FortiAP Manager

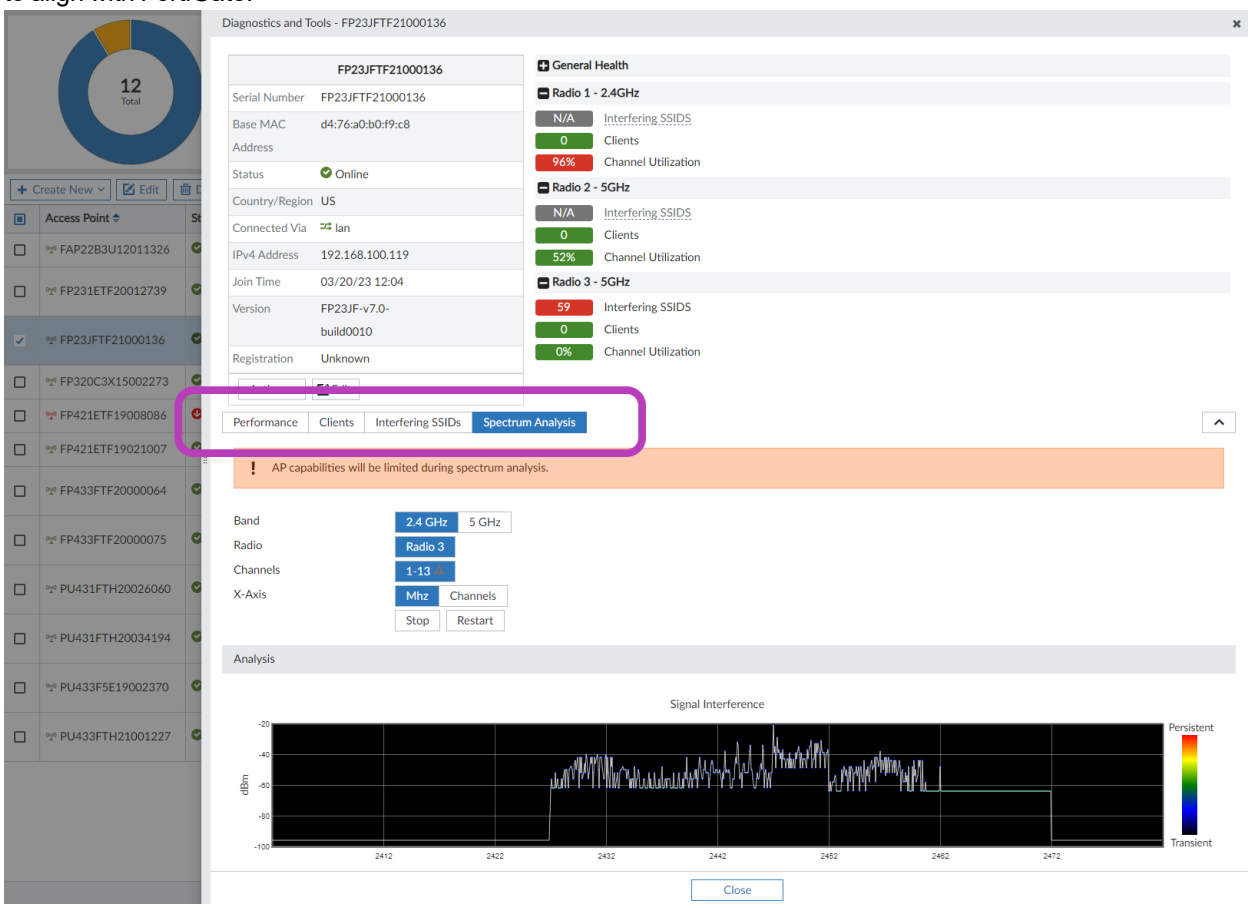
- The different graphics, colors, and icons in FortiManager are aligned with the design of FortiGate. The changes include graphics, AP icon, channel utilization, diagnostics and tools, and AP groups.



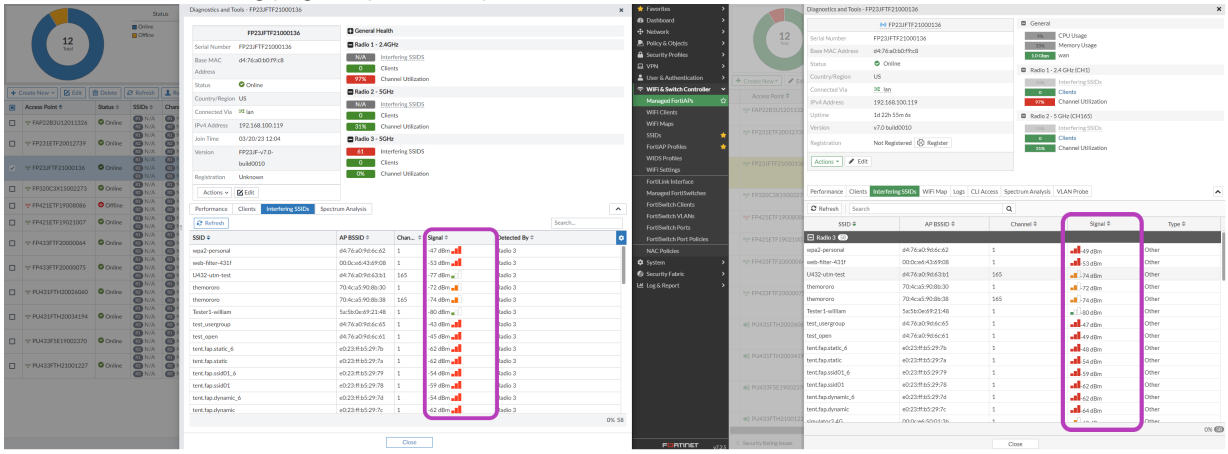
- AP Groups are not shown in the table view by default. You can enable it by going to *List* > *Group* in the toolbar.



- An empty space under the *Diagnostics and Tools* menu no longer exists, and the *Summary* tab has been removed to align with FortiGate.

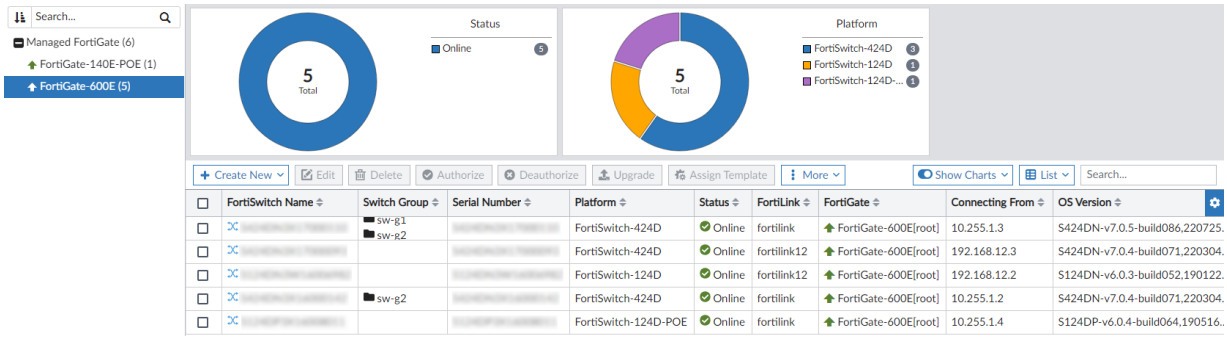


- On the client monitoring page, *Signal Strength* and *Rate Calculation* issues are resolved.

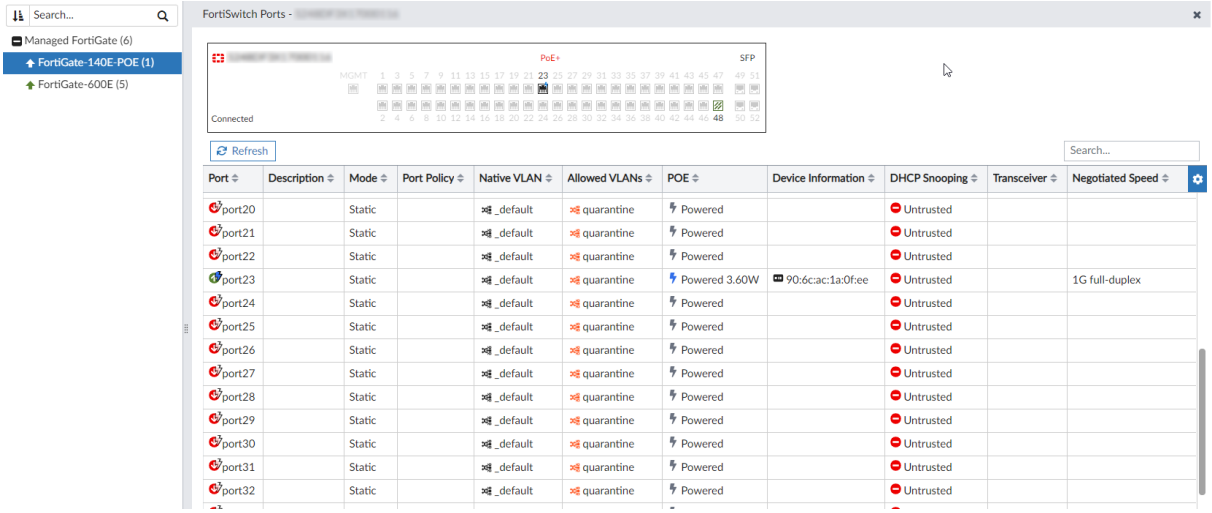


FortiSwitch Manager

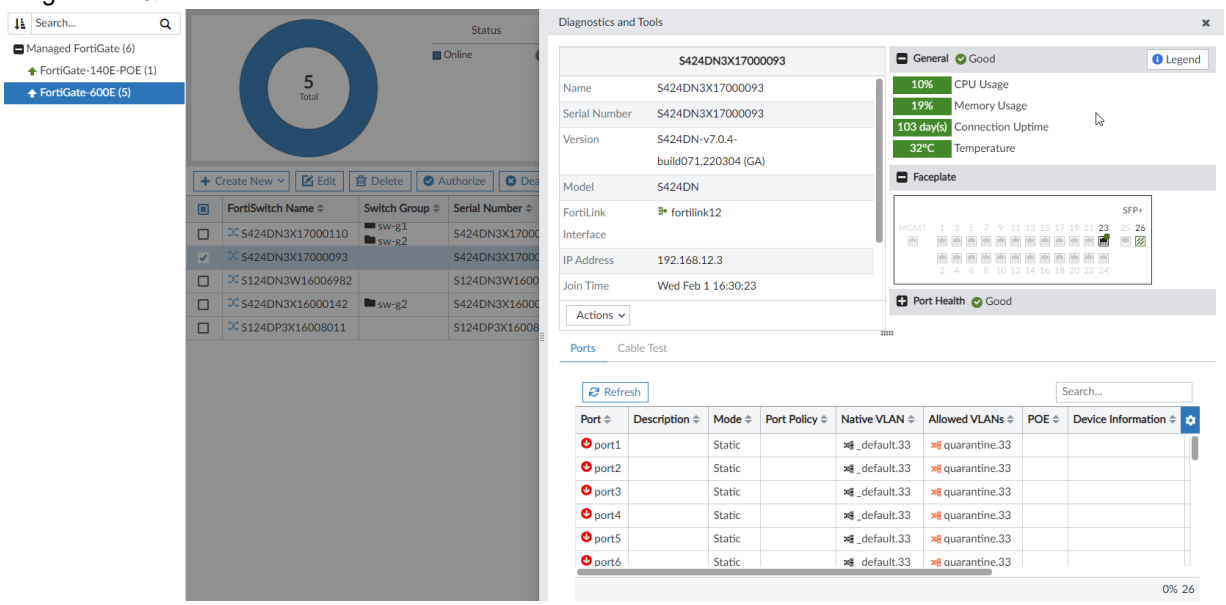
- Enhancements have been made to the layout of the FortiSwitch Manager page.
  - General.



  - FortiSwitch Ports.



- Diagnostics & Tools.



FortiManager imports EPGs entries using the Cisco ACI connector as individual objects

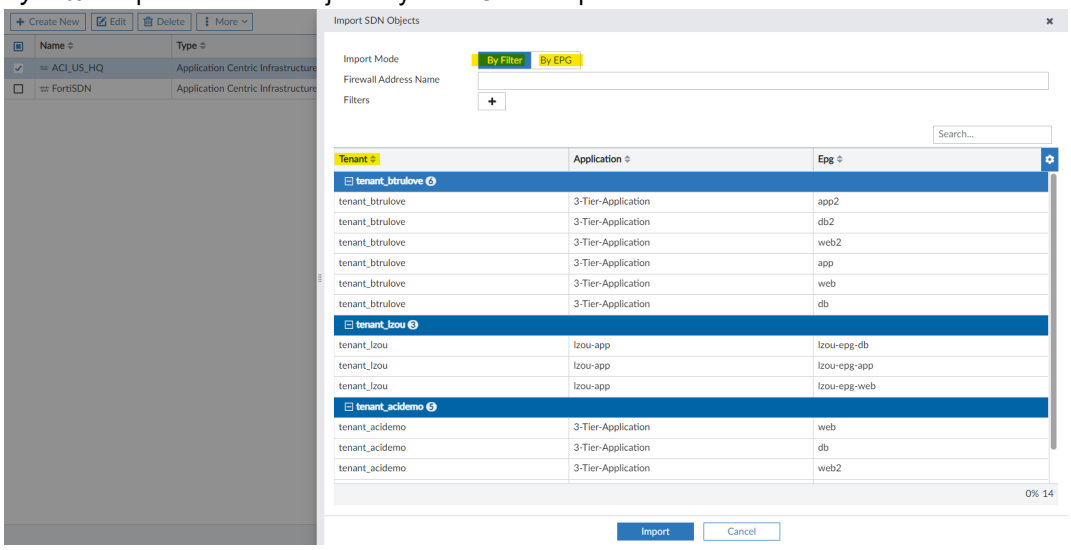
FortiManager imports EPGs entries using the Cisco ACI connector as individual objects.

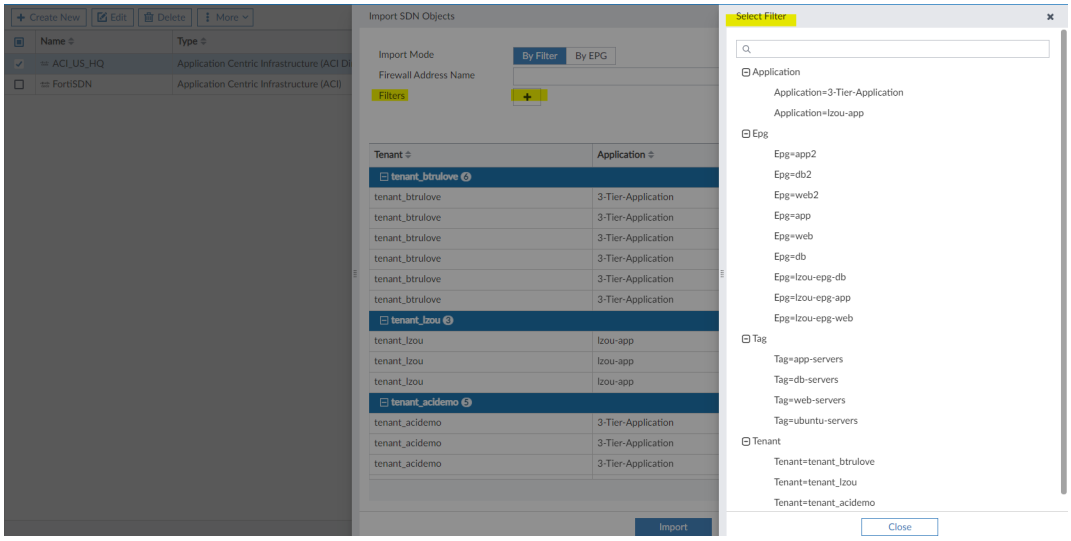
In order to import Endpoint Groups (EPGs) from ACI using the process described below, you must have already configured your Cisco APIC server.

To import EPGs as standalone objects from an ACI connector:

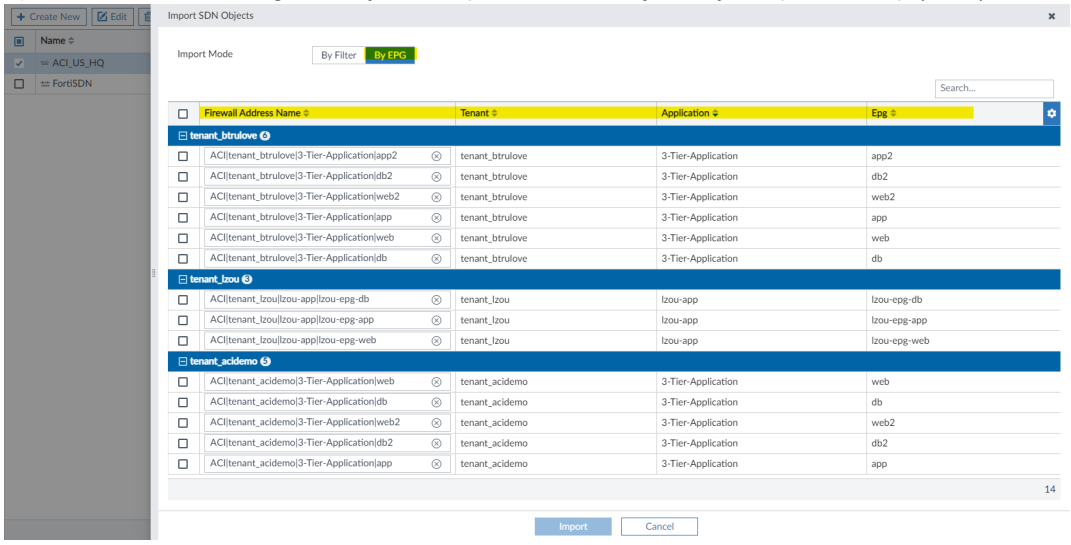
1. In FortiManager, configure the Application Centric Infrastructure (ACI) connector to use the *Direct Connection* ACI Type.
2. After configuring the remaining connector settings, you can import the SDN objects from *Policy & Objects* > *Object Configurations* > *External Connectors* > *Private SDN*, by right-clicking on the newly created Cisco ACI connector and choosing *Import*.
   The import function loads all objects from the APIC server.

3. In the *Import SDN Objects* dialog, the *Import Mode* setting includes two modes: *By Filter* and *By EPG*.
   - *By Filter*: Imports the SDN objects by filter. Click the plus icon to add filters.

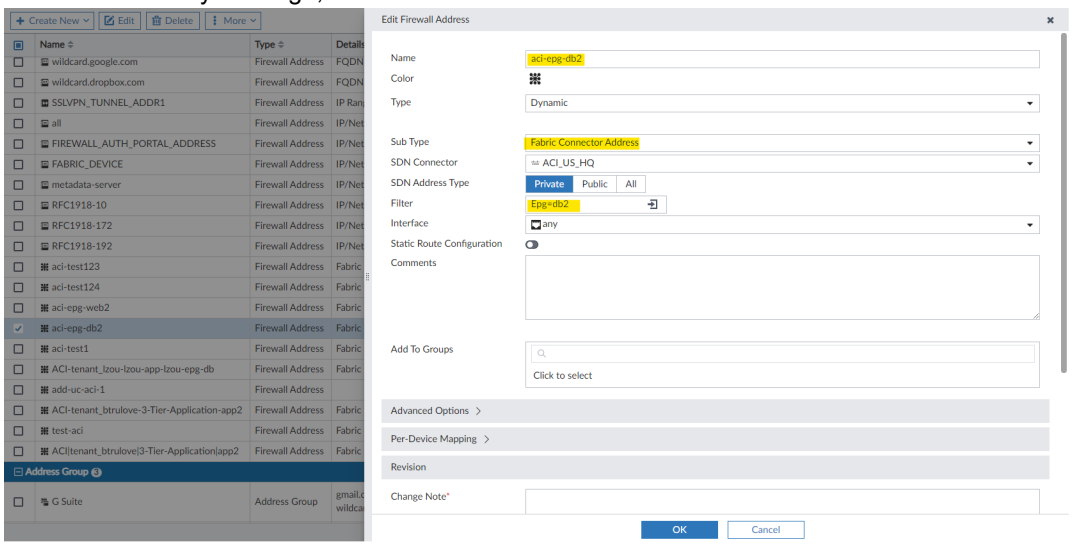


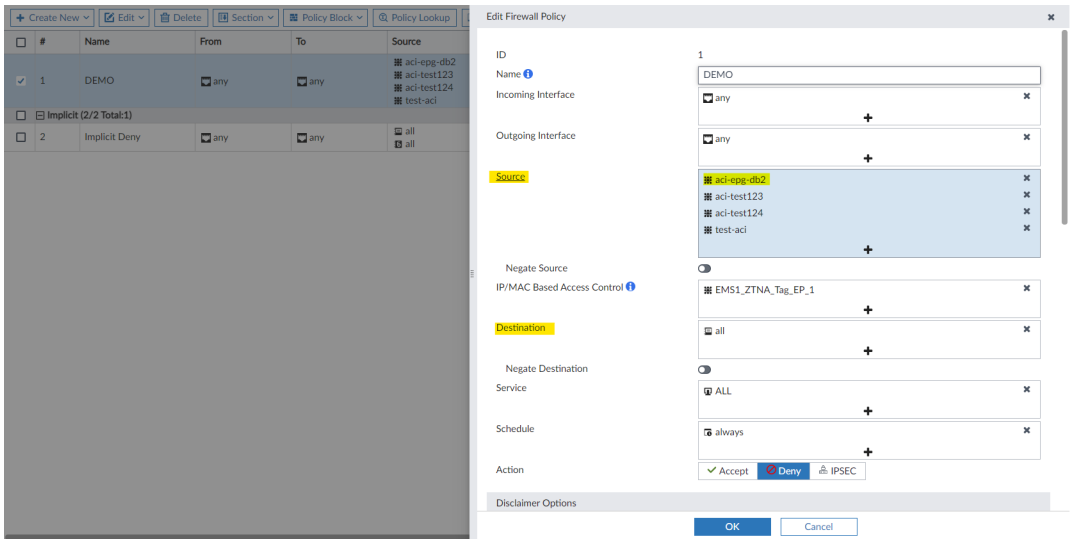


- *By EPG*: This new setting allows you to import the SDN objects by Endpoint Group (EPG).



4. You can create address objects from *Policy & Objects* > *Object Configurations* > *Firewall Objects* and use the address in a Policy Package, similar to other SDN connectors.




Create New
Edit
Delete
Section
Policy Block
Policy Lookup
#
Name
From
To
Source
1
DEMO
any
any
aci-epg-db2
aci-test123
aci-test124
test-aci
Implicit (2/2 Total:1)
2
Implicit Deny
any
any
all
all
Edit Firewall Policy
ID
1
Name
DEMO
Incoming Interface
any
Outgoing Interface
any
Source
aci-epg-db2
aci-test123
aci-test124
test-aci
Negate Source
IP/MAC Based Access Control
EMS1_ZTNA_Tag_EP_1
Destination
all
Negate Destination
Service
ALL
Schedule
always
Action
Accept
Deny
IPSEC
Disclaimer Options
OK
Cancel

Index

The following index provides a list of all new features added to FortiManager 7.4. The index allows you to quickly identify the version where the feature first became available in FortiManager.

Select a version number to navigate in the index to the new features available for that release:

7.4.0

Device Manager

SD-WAN	• Automated SD-WAN post overlay process creates policies to allow the health-checks traffic to flow between Branch and HUB on page 12 • Automated SD-WAN overlay process adds "branch_id" meta variable auto assignment on page 15 • SD-WAN monitoring map integrates with Cloud Assisted Monitoring Service to allow FortiGate interface speed tests from inside FortiManager on page 16 • SDWAN monitoring map enhancements on page 19 • SDWAN template for heterogeneous WAN link types on page 23
Templates	• Preview CLI configuration for the device provisioning templates on page 25 • Fortinet factory-default wireless and extender templates on page 28 • Jinja Templates have direct access to the device DB to support generation of dynamic configuration on page 34

Central Management

FortiSwitch Manager	• Per-device VRRP mapping can be used under FortiSwitch Profiles on page 50 • FortiManager allows switchport export to another VDOM, and configuration of the exported port in the destination VDOM on page 51 • FortiSwitch replacement procedure can be executed from FortiManager GUI on page 54
Other enhancements	• FortiManager supports install preview for model devices on page 59 • VPN Monitoring displays IPsec VPN tunnels created by IPsec templates and SD-WAN overlay wizard on page 64 • FortiManager supports CLI diff in the workflow approval sessions on page 67

Policy and Objects

Policy	• Install preview support for partial install on page 71 • Policy Package installation added link to the progress report page for installation errors on page 78 • Support for IoT Virtual Patching in NAC policies using pre-built severity filters on page 82

System

High availability	• FortiManager supports different VM type platforms to form the FortiManager cluster on page 92
Other enhancements	• Block out contract device from upgrading to next or major or minor release on page 100

Cloud Services

Cloud services	• FortiManager used as single-pane management tool to orchestrate FortiGate deployment in AWS on page 105

Other

Other enhancements	• New FortiManager UX design on page 111 • Fabric and External connector pages have been reorganized for an enhanced user experience on page 121 • FortiManager connector relay to AWS will proxy all individual FortiGate requests on page 125 • FortiManager key areas have been reorganized to enhance user experience on page 126 • FortiManager imports EPGs entries using the Cisco ACI connector as individual objects on page 140

7.4.1

Device Manager

Device and groups	• Auto-link setting is exposed to control configuration installation during ZTP 7.4.1 on page 8
Templates	• Fabric Authorization Template is integrated with Device Blueprint and supports meta variables 7.4.1 on page 41

Central Management

Policy and Objects

System

www.fortinet.com